Subject: Electronic CIPHER, Issue 27, April 27,

```
    _/_/_/_/  _/_/_/  _/_/_/_/  _/    _/  _/_/_/_/  _/_/_/_/
   _/          _/    _/    _/  _/    _/  _/        _/    _/
  _/          _/    _/_/_/_/  _/_/_/_/  _/_/      _/_/_/_/
 _/          _/    _/        _/    _/  _/        _/  _/
_/_/_/_/  _/_/_/  _/        _/    _/  _/_/_/_/  _/    _/
```

==
Newsletter of the IEEE Computer Society's TC on Security and Privacy
Electronic Issue 27   April 27, 1998
Avi Rubin and Paul Syverson, Editors
                              Bob Bruen, Book Review Editor
                              Hilarie Orman, Assoc. Editor
                              Mary Ellen Zurko, Assoc. Editor
                              Anish Mathuria, Reader's Guide
==
        http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/

Contents: [3354 lines total]

Letter from the TC Chair

In about a week, the Technical Committee will host its flagship conference, the annual Symposium on Security and Privacy. For the nineteenth year this conference will be held in Oakland, California, at the Claremont Hotel. This conference attracts researchers, practitioners, and students from around the world for 2-1/2 days of papers and panels. For many people the most important part of the conference is the opportunity for informal discussions among security professionals on the state of our profession.

But the purpose of this column now is not to focus on this years conference, which may even be over by the time you read this. Instead I want to put in a plug for next years conference, which will be held on 9-12 May, 1999. 1999 will be the twentieth year of this conference. The conference chair, John McLean, and the senior program co-chair, Li Gong, are already thinking of some ways in which we can celebrate this significant anniversary.

You can help us with this celebration in two ways. First, please begin now to make your plans to attend this special conference. Mark your

calendar for 9-12 May 1999. Start to work on the paper you want to
submit, begin to arrange funding, and organize your schedule. Second,
help us to make this conference distinctive. Perhaps you are involved
in some activity for which a workshop of your colleagues would be
helpful. Think of scheduling your workshop in Oakland before or after
the symposium. Maybe you have an idea for a new event that would be
interesting at the conference. In recent years we have added birds of
a feather sessions, five-minute talks, and book displays. The
conference organizers are always interested in refining the conference
to improve it. Can you think of a way in which we can make this
twentieth conference really distinctive? Please let us know.

I hope you will begin planning for next years conference, as we are
already. Details on the conference will appear in Cipher as they
become available. Please help us make it a truly outstanding event.

Charles P. Pfleeger
Chair, TC on Security and Privacy

Letter from the Editor

Dear Readers,

It is time once again to bring you an issue of Cipher. In
this issue, you'll find information about the two primary IEEE
sponsored conferences in security, some news reports, trip
reports, calendendar information and much more.

As you can see, we are starting to see consolidation in the
computer security industry. It will be interesting to see who
the big winners and losers are as bigger companies gobble up
smaller ones, and others merge together. In the latest round,
Network Associates, the same company that bought PGP Inc.,
purchased Trusted Information Systems. Meanwhile, the encryption
debate continues to rage on the hill, more and more crypto is
developed internationally, and it's deja vu all over again.

Once again we'd like to thank all of the contributors who make
this newsletter possible, especially all of our associate editors,

who do the real work behind this "publication". Also, thanks
to Carl Landwehr for continuing guidance and helpful suggestions.

Avi Rubin and Paul Syverson
Editors, Cipher

FINAL PROGRAM AND REGISTRATION INFORMATION:
1998 IEEE Symposium on Security and Privacy

```
1998 IEEE SYMPOSIUM ON SECURITY AND PRIVACY        _/_/
                         _/    _/
                        _/     _/
May 3-6, 1998                 _/_/  _/_/_/
The Claremont Resort              _/  _/
Oakland, California           _/ _/
                        _/_/
Sponsored by the                 _/_/_/
IEEE Technical Committee on Security and Privacy     _/  _/
In cooperation with the          _/  _/
International Association of Cryptologic Research     _/_/_/
                          _/
Symposium Committee               _/
Michael Reiter, General Chair       _/_/_/  _/_/_/
John McLean, Vice Chair            _/  _/ _/   _/
Paul Karger, Program Co-Chair       _/  _/ _/   _/
Li Gong, Program Co-Chair          _/_/_/ _/_/_/
                            _/ _/   _/
           PRELIMINARY PROGRAM          _/ _/   _/
            Subject to Change   _/ _/_/_/
```

Sunday May 3, 1998

4:00-7:00 Registration and Reception

Monday May 4, 1998

8:00 Registration
8:45 Introductory Remarks
9:00 - 10:30 Access Control

Access Control in an Open, Distributed Environment
Jean Bacon (Cambridge University), Richard Hayton (APM Ltd.),
and Ken Moody (Cambridge University)

Ensuring Continuity During Dynamic Security Policy Reconfiguration in DTE
Timothy Fraser and Lee Badger (Trusted Information Systems)

Composing Partially-Specified Systems
Heather M. Hinton (Ryerson Polytechnic University)

10:30-11:00 Break

11:00-12:00 Java Security

Secure Execution of Java Applets using a Remote Playground
Dahlia Malkhi, Michael Reiter, and Aviel Rubin (AT&T Labs - Research)

Understanding Java Stack Inspection
Dan S. Wallach and Edward W. Felten (Princeton University)

12:00-2:00 Lunch

2:00-3:30 Cryptography I

Efficient Key Distribution for Slow Computing Devices:
Achieving Fast Over the Air Activation for Wireless Systems
Yair Frankel (CertCo), Chris Carroll and
Yiannis Tsiounis (GTE Laboratories)

Efficient and Practical Fair Exchange Protocols with Off-Line TTP
Feng Bao, Robert Deng (National University of Singapore) and
Wenbo Mao (HP Laboratories, Bristol)

Asynchronous Protocols for Optimistic Fair Exchange
N. Asokan, V. Shoup, and M. Waidner (IBM Research, Zurich)

3:30-4:00 Break

4:00-5:00 Panel: Trust Considerations in PKI Systems
Moderator: Dale Johnson (MITRE)
Panelists: TBA

6:00-7:30 Reception

Tuesday May 5, 1998

9:00-10:30 Architectures

An Automated Approach for Identifying Potential Vulnerabilities in Software
Anup K. Ghosh, Tom O'Connor, and Gary McGraw
(Reliable Software Technologies)

Detecting Disruptive Routers: A Distributed Network Monitoring Approach
Kirk A. Bradley, Biswanath Mukherjee, Ronald A. Olsson, Nick Puketza
(University of California at Davis)

Timing Attacks Against Trusted Path
Jonathon T. Trostle

10:30-11:00 Break

11:00-12:00 Database Security and Biometrics

Partial Security Policies to Support Timeliness in
Secure Real-Time Databases
Sang Son, Craig Chaney, and Norris Thomlinson (University of Virginia)

On Enabling Secure Applications Through Off-Line Biometric Identification
George I. Davida (Univ. of Wisconsin, Milwaukee),
Yair Frankel (CertCo) and Brian J. Matt (Sandia National Laboratories)

12:00-2:00 Lunch

2:00-3:30 5-Minute Talks

3:30-4:00 Break

4:00-5:00 Formal Methods I

Strand Spaces: Why is a Security Protocol Correct?
F. Javier Thayer Fabrega, Jonathon C. Herzog,
and Joshua D. Guttman (MITRE)

On the Formal Definition of Separation-of-Duty Policies
and their Composition
Virgil D. Gligor (University of Maryland),
Serban I. Gavrila (VDG, Inc.), and David Ferraiolo (NIST)

5:00-6:00 Meeting, Technical Committee on Security and Privacy

Wednesday May 6, 1998

9:00-10:00 Formal Methods II

Complete, Safe Information Flow with Decentralized Labels
Andrew Myers and Barbara Liskov (MIT)

Stack and Queue Integrity on Hostile Platforms
Prem Devanbu (Univ. of Calif. at Davis) and
Stuart Stubblebine (AT&T Labs - Research)

10:00-10:30 Break

10:30-11:30 Cryptography II

Necessity and Realization of Universally Verifiable Secret Sharing
Wenbo Mao (HP Laboratories, Bristol)

Towards Mobile Cryptography
Tomas Sander and Christian F. Tschudin
(Intl. Computer Science Inst., Berkeley, CA)

11:30-12:00 Presentation of Awards and Announcement of New TC Officers

```
--------------------
1998 IEEE SYMPOSIUM ON SECURITY AND PRIVACY                _/_/
                              _/    _/
        REGISTRATION FORM               _/       _/
                              _/_/   _/_/_/
    Name:____________________________________________    _/   _/
                            _/   _/
  Affiliation:_____________________________________________  _/_/
                              _/_/_/
```

Postal Address:____ _/ _/
_/ _/
____ _/_/_/
_/
____ _/
_/_/_/ _/_/_/
Phone:____ _/ _/ _/ _/
_/ _/ _/ _/
Fax:____ _/_/_/ _/_/_/
_/ _/ _/
Email:____ _/ _/ _/
_/ _/_/_/

Note: Address information will be distributed to attendees.

Please enter the appropriate registration category. Payment must be
included and must be either by check in U.S. dollars, drawn on a U.S.
bank and made payable to "IEEE Symposium on Security and Privacy", or
by credit card. Dates are strictly enforced by postmark.

Advance registration (up to 28 March 1998)
___ Member, IEEE or Computer Society (Member #__________, required).$310.00
___ Non-Member...$385.00
___ Full-time Student...$100.00
Late registration (from 29 March 1998)
___ Member, IEEE or Computer Society (Member #__________, required).$370.00
___ Non-Member...$460.00
___ Full-time Student...$100.00

Do you wish to present at a poster session or lead an evening discussion?

[ ] Yes [ ] No

Do you have any special requirements?____

Please indicate your method of payment by checking the appropriate box:

[ ] Check in U.S. funds drawn on a U.S. bank (PLEASE ENCLOSE WITH THIS FORM)

Credit card authorization:
(Charges will appear on your statement as made by IEEE COMPUTER SOCIETY.
Note: your credit card number will be transmitted to the IEEE over the

Internet, using an SSL-protected link.)

Visa MasterCard American Express Diners Club
[ ] [ ] [ ] [ ]

Credit Card Number:____

Card Holder Name:_____________________________Expiration Date:____________

Signature (required for credit card payments):_____________________________

Mail registration to:
John McLean
Naval Research Laboratory
Code 5540
4555 Overlook Avenue, SW
Washington, DC 20375-5337

Or FAX this form (CREDIT CARD
REGISTRATIONS ONLY) to:
FAX: +1 202 404-7942
VOICE: +1 202 404-8888

>>>>SORRY, NO REGISTRATIONS BY EMAIL. NO REFUNDS.<<<<

Evening Sessions
================

The 1998 IEEE Symposium on Security and Privacy will accommodate poster sessions and evening discussions. There will be rooms for interested parties to post presentations on work in progress, recent research results, and innovative proposals, or to lead discussions on topics of current interest. These rooms will be available Monday and Tuesday, May 4 and 5. If you are interested in posting a presentation or organizing a discussion on a particular topic, please indicate so on the registration form.

Hotel Reservations - The Claremont Resort
===

The Claremont Resort in Oakland, California is situated in the Oakland-Berkeley hills overlooking the San Francisco Bay on 22 acres of beautifully landscaped lawns and gardens. Facilities include the Claremont Pool and Tennis Club and The Spa at the Claremont.

To reach the hotel, allow 35 minutes from the Oakland Airport and 45 minutes from the San Francisco Airport. Bayporter Express (+1 415 467-1800) provides shuttle service from either airport to the

Claremont Resort. The charge is $12 from the Oakland Airport and $13 from the San Francisco Airport, per person one way. Parking is available at the hotel at a cost of $8 per day for guests and a maximum of $9 per day for non-guests.

Hotel reservations must be made under the group name IEEE Symposium on Security and Privacy. The group rate is $121 single, $133 double occupancy, plus 11% tax. These rates are available for the period May 1-8, 1998. The cut-off date for reservations is Wednesday, April 1, 1998. Reservations made after this date will be accepted on a space available basis. Reservations must be accompanied by an advance deposit or credit card guarantee. Individual cancellations will be accepted 24 hours prior to the check-in date. Please be advised the check-in time is after 3:00 p.m.; check-out is 12 noon.

For reservations and information, contact: The Claremont Resort, Ashby and Domingo Avenues, Oakland, CA 94623-0363; Phone: +1 800 551-7266 (7 a.m. to 8:30 p.m., PST) or +1 510 843-3000; Fax: +1 510 549-8582.

PRELIMINARY PROGRAM FOR CSFW11
(the IEEE Computer Security Foundations Workshop)

(Conference Web page http://www.csl.sri.com/~millen/csfw/)

11th IEEE Computer Security Foundations Workshop
June 9-11, 1998
Rockport, Massachusetts, USA
Sponsored by the IEEE Computer Society

Technical Program

Tuesday, June 9, 1998
================

8:50-9:00 Welcome
Simon Foley (Program Chair) &
Jonathan Millen (General Chair).

9:00-10:30 Session 1: Distributed Services
Chair: Li Gong

Weakly Secret Bit Commitment: Applications to Lotteries
and Fair Exchange
P. Syverson (Naval Research Laboratory)

On the Structure of Delegation Networks
T. Aura (Helsinki University of Technology)

Two Facets of Authentication
M. Abadi (DEC Systems Research Center)

10:30-11:00 Coffeebreak

11:00-12:00 Session 2: Noninterference
Chair: E.S. Lee

Probabilistic Noninterference in a Concurrent Language
D. Volpano (Naval Postgraduate School),
G. Smith (Florida International University)

Partial Model Checking and Theorem Proving for
Ensuring Security Properties
F. Martinelli (Universita di Siena & Universita di Pisa)

12:00-14:00 Lunch

14:00-15:30 Session 3: Protocol Verification
Chair: Catherine Meadows

Formal Analysis of a Non-repudiation Protocol
S. Schneider (University of London, RHBNC)

Honest Ideals on Strand Spaces
J. Thayer, J. Herzog, J. Guttman (MITRE Corporation)

15:00-15:30 Coffeebreak

15:30-17:30 Panel 1: Varieties of Authentication
Moderators: R. Gorrieri (University of Bologna)
& P. Syverson (Naval Research Laboratory)
Panel Members: M. Abadi, R. Focardi, G. Lowe,
C. Meadows, D. Gollmann

```
18:30-21:30     Dinner

Wednesday, June 10, 1998
======================

9:00-10:30      Session 4: Protocol Model Checking
                Chair: Jonathan Millen

Proving Security Protocols with Model Checkers by
Data Independence Techniques
A.W. Roscoe (University of Oxford)

Towards a Completeness Result for Model Checking of
Security Protocols (Extended Abstract)
G. Lowe (University of Leicester)

Efficient Finite-State Analysis for Large Security Protocols
V. Shmatikov and U. Stern (Stanford University)

10:30-11:00     Coffeebreak

11:00-12:00     Session 5: Composition
                Chair:

Composing Secure Systems that have Emergent Properties
A. Zakinthinos (ACCSL) & E.S. Lee (University of Cambridge)

Merging security policies: analysis of a practical example
F. Cuppens, L. Cholvy, C. Saurel, J Carrere (ONERA-CERT)

12:00-14:00     Lunch

14:00-15:00     Session 6: Protocol Logics
                Chair: Gavin Lowe

Evaluating and Improving Protocol Analysis by Automatic Proof
S. Brackin (Arca Systems)

A Simple Logic for Authentication Protocol Design
L. Buttyan and S. Staamann (Swiss Federal Institute of Technology)
```

15:00-15:30 Coffeebreak

15:30-17:30 Panel 2: The Security Impact of Open/Distributed
Computing Technologies
Moderator: P Ryan (Defence Research Agency)
Panel Members: TBA

18:30-21:30 Dinner

Thursday, June 11 1998
======================

9:00-10:30 Session 7: Database and Intrusion Detection
Chair: Robert Morris

A Fair Locking Protocol for Multilevel Secure Databases
S. Jajodia (George Mason), L. Mancini (Universita La Sapienza
di Roma), S. Setia (George Mason)

Data Level Inference Detection -- A Rule Based Approach
R. Yip, K. Levitt (University of California, Davis)

Abstraction-Based Misuse Detection: High-Level
Specifications and Adaptable Strategies
J-L. Lin, X.S. Wang S. Jajodia (George Mason)

11:00 Coffeebreak

11:00-12:00 Business Meeting.

SECURITY AND PRIVACY SURVEY BY THE IEEE COMPUTER SOCIETY

The IEEE Computer Society is conducting a survey to determine how its members (and others) feel about various matters primarily relating to government regulation of export and use of cryptography. Readers wishing to take part will find a clickable on-line form at http://ada.computer.org/surveys/Privsec.htm

---

SECURITY AND PRIVACY NEWS BRIEFS

LISTWATCH: items from security-related mailing lists (4/21/98)
by Mary Ellen Zurko, The Open Group Research Institute
(m.zurko@opengroup.org)

This issue's highlights are from risks, tls, cypherpunks, dcsb, spki, tbtf, e-carm, e$, and digsig.

Commerce Secretary William M. Daley said that the current controls on encryption technology are hurting America's ability to compete with other countries. "There are solutions out there. Solutions that would meet some of law enforcement's needs without compromising the concerns of the privacy and business communities. But I fear our search has thus far been more symbolic than sincere..." One rumored industrial compromise is to hold the line on transmitted data, but to give some on stored data in exchange for concensions on export controls.

The digital cellular phone encryption system, GSM, was cracked by two researchers at UC Berkeley. They managed to crack the code on the SIM or smart card, which does not seem to be radio-transmitted information. They repeatedly asked the card to identify itself, and so cracked it by brute force. See the web site http://www.isaac.cs.berkeley.edu/isaac/gsm.html for more information. The Time article says: ``What was even more intriguing than the security threat, however, was that cracking the code yielded a tantalizing hint that a digital key used by GSM may have been intentionally weakened during the design process to permit government agencies to eavesdrop on cellular telephone conversations." The 64 bit key seems to have 10 bits that are always zero. A Risks contributer stated that that was no news; the use of GSM in Australia was blocked on the day of the official launch because the security and police services wanted an easier code to break. One of the Berkeley researchers indicated that he thought it was the choice of algorithm, not the key length, that had been weakened in the design phase.

On the TLS working group list, there is a discussion (again) of whether to allow the null ciphersuite (no security) as a negotiable option. The motivating example is a printer available with and without security, and the desire to list it on only one port. The protocol is susceptable to an active downgrade attack, and if both parties support this option they could be coerced to communicate in the clear.

Rivest sparked discussion on spki on the topic of revocations, by proposing certificates carry an issue ("not before") date, a "good until" date (guarantted; no revocation before then), and an expiration date.

An S/MIME Freeware Library was announced. More information can be found at http://www.imc.org/imc-sfl/.

Within 15 hours of Netscape's release of the freeware source for their browser, the Austrailian-led Mozilla Crypto Group (http://mozilla-crypto.ssleay.org) had put the crypto back into the source code. The reports are unclear about just how functional the first pass of this was, but the intent of the group is clear.

An anonymous poster to cypherpunks announced "Weaken" for Netscape, inspired by the Fortify efforts that strengthen a Netscape browser's security capabilities. Their points seemed to be: it's hard to verify that Fortify works and that weakening the browser makes a great virus.

While the technical content of the latest discussion on e-carm on determining whether a public key signature is valid (not compromised) is probably familiar to many readers, I found it interesting that proponents of electronic commerce didn't bat an electronic eye when a poster stated that the issue of who is responsible for the losses incurred from a forgery would probably get resolved over time, by case law. There's been a lot of talk in the e-commerce community about making users feel comfortable (secure, if you will :-) with electronic commerce. Statements like that will keep consumers away in droves.

Seiko is going to start selling wristwatch PC's in June. They can exchange data with each other through infrared signals. The first version seems targeted at games, which seems like a good market to go after if you aren't ready to deal with the security implications. I'd love to see these start appearing as personal calendaring appliances, particularly when funders visit :-).

A rumor from the crypto import trenches in Russia: while importing crypto requires a license, there are serveral license authorities, and at least one of them gives license freely. I wonder if they make more money that way.

A European ecommerce developer stated that he had been frustrated in his efforts to deploy ecommerce for European banks because they insist on waiting for SET.

There is an interesting dicussion on e-carm about whether there is a business for CAs. Interestingly, some participants claim that having a business in the middle only weakens security. My discussions with acquaintances at businesses selling CA services indicate to me that they pay enormous attention to security, and have the ability to attrack and keep top talent in that area because of the concentration of interesting security issues. Discussion also included other issues such as investment. At about the same time, participants on digsig where discussing whether a hierarchical CA model could work (for banks) at all, with Bob Hettinga championing more geodesic structures.

A New York Times article announced a weakness in 3DES (http://jya.com/3des-weak.htm). Schneier pointed out that the attack is only against a particular mode in the standard and requires something like 2^64 texts. It is not a practical attack.

Rivest announced a new notion in encryption, Chaffing and Winnowing (http://theory.lcs.mit.edu/~rivest/chaffing.txt), which uses authentication only to hide information. The basic notion is that multiple reasonable versions of each packet of information are sent, but only the one that authenticates properly is the right one. Taking packets down to communicating one bit each gives excellent privacy, at the expense of a great deal of bandwidth. As Rivest and other point out, this technique has a lot in common with steganography. It's raison d'etre is to indicate the futility of restrictions on cryptography, in part because the adding of chaff (extra packets) can be done by any party between the sender and receiver. Several discussants pointed out that similar schemes had been suggested in the past.

Cypherpunks continued to consider what Network Associates (NAI) will do with PGP and TIS, two companies who security philosophy seems diametrically opposed (NAI announced its plans to buy TIS since the last issue of Cipher). Opinions range from those who believe PGP will be milked of its good name and disposed of, to those that believe TIS will be used as a firewall and sop to government customers. No one has proposed a specific innovative blending of the two companies' products. Zimmerman issued a strong yet vague statement, saying that NAI does not plan to put key escrow in PGP, that his political views on crypto and privacy have not changed, and that he did not sell his company to see it buried.

Network Associates in Europe is said to be shipping strong PGP. It claims to not have broken US laws, since its US operations did not do anything to help the european effort (which was accomplished by having Cnlab Software in Switzerland produce the code). It was unclear if Cnlab started with the book-form scannable version of PGP that was legally exported.

Sun's efforts to sell strong crypto overseas by using the code that the Russian firm Elvis developed, are officially stalled due to "ongoing scrutiny by the US Commerce Department" (Wired). I'm sure this resonates with anyone who's been involved with attempting to export crypto.

The April 1st Risks was a classic. Here are my favorites:

Date: Wed, 1 Apr 1998 -8:00:00 -0800
From: Douglas Moran <moran@ai.sri.com>
Subject: Funding for a new software paradigm

(Washington, DC, press release by IP Newswire, 1 April 1998) The Defense Advanced Research Projects Agency (DARPA) today announced a major new initiative in software engineering. F.P. Rivers, program manager for the initiative, said that it addresses a major problem facing the US military: that much of current information technology is too "compute-intensive" to be deployed where it is most needed -- at the small unit or even individual soldier level.

This initiative has its origins in a fortuitous observation: Rivers and several colleagues noticed that users on the most widely used platform -- Windows 95 -- were routinely presented with messages that an unknown unrecoverable error had occurred, and that these users just as routinely ignored those messages. "This occurred not just in casual use, but also in mission-critical operations."

Rivers said, "Once we started thinking about these messages not as a help, but as a hindrance, several other observations came together." In a typical program, 40% to 80% of the code is devoted to error detection and error handling. "Software bloat" -- the ever increasing size of programs -- has been blamed on programmers adding more and more features, but could also be blamed on all the error handling associated with those features. To make matters worse, multiple studies had shown that much, if not most, of the error-handling code was never tested. Sometimes this was because of time and budget pressures; sometimes the potential errors were so obscure and complex that the situations were too difficult to create "in the lab". This research was backed up by actual experience: error-handling code was often found to have significant errors.

Rivers summarized, "So, the typical program is overloaded with code that is rarely used, that may not work, and whose output is likely to be ignored anyway." He concluded, "With this code removed, programs will be dramatically smaller and will run somewhat-to-noticeably faster."

Many software developers, including several major vendors, have already taken some tentative steps in this direction, having recognized pieces of the problem, but without grasping the "big picture". Rivers said he expects this new approach, dubbed "Fault-Oblivious Computing", to quickly become the dominant software-engineering paradigm. He acknowledged that there were small highly specialized segments where fault-tolerant computing and program verification would still be of value. A major component of this initiative will be to develop tools to automatically identify and remove unneeded error-handling code from existing applications.

The success of this approach would be be bad news for memory-chip manufacturers, who are already hard-hit by decreased demand.

[Perhaps Fault-Oblivious Computing could be used to help with the Y2K problem, getting rid of all those gratuitous date comparisons!!! PGN]

Date: Wed, 1 Apr 1998 -05:00:00 -0500
From: andrew@greenehouse.com
Subject: Quantum computer cracks crypto keys quickly

A small team of researchers has succeeded in building a prototype of the so-called "quantum computer" that can factor large numbers quickly and defeat public-key cryptosystems.

The researchers cracked the DES-IV-1 challenge, revealing the message "Can't anyone around here keep a secret?"

Since the new computer is based on superconducting quantum interference devices, it is not bound by conventional temporal limits on computation. In fact, the researchers were able to use their system to crack challenges that had not yet been created. These future secret messages included, "God in Heaven, what have we done?" and the cryptic "tsopyadslooflirpanasisihtsey" -- which clearly shows that future challenges are going to use multiple layers of encryption.

President Clinton congratulated the researchers, but said that he was considering a proposal to ban the export of quarks from the United States until the NSA could implement a quark escrow system, by which each quark in the universe would be uniquely numbered.

When asked if their invention would enable scientists to foretell the future, the researchers pointed out that they can only decrypt messages that are encrypted using certain methods that are known today. Furthermore, there is no way for them to determine if the messages that they receive are authentic or if unknown people are sending false messages to confuse us.

"If only there were a reliable way to digitally sign a transmission," bemoaned one of the researchers.

An Update from Asia by Yongfei Han

Ciphers and Security in Asia

The international Conference on Information and Communications Security (ICICS) was successfully hold in Beijing, P. R. China, in November 11-14, 1997, with around 180 participants from 23 nations. There were 87 papers submitted for inclusion, from an international authorship, 37 papers among them have been accepted as regular papers, and 11 as short papers. The proceedings, Lecture Notes in Computer Science 1334, were distributed at the conference. The program co-chair were Yongfei Han, Tatsuaki Okamoto and Sihan Qing.

The steering committee of the ICICS, where now the members are Chin-Chen Chang, James W. Gray, III, Yongfei Han, Kwangjo Kim, Tatsuaki Okamoto, Sihan Qing and Vijay Varadharajan, has decided that ICICS '99 will be in Sydney, Australia. The program co-chair will be Vijay Varadharajan and Josef Pieprzyk. The committee will get more members before the end of 1997.

The steering committee of AsiaCrypto, where now the members are Prof. Imai, Dr. T. Okamoto, Prof. E. Okamoto, Prof. T. Matsumoto, Prof. Vijay Varadharajan, Prof. Josef Pieprzyk, Prof. Ed Dawson, Prof. S. Qing, Prof. D. Pei, Drs. Yongfei and K. Lam, and Dr. K, Kim, etc, has decided that AsiaCrypt '99 will be in Singapore and the general chair will be Drs. K. Lam and Yongfei Han. AsiaCrypt '2000 will be in Japan. AsiaCrypt '98 will be in Beijing the CFP can be found by http://www.iacr.org.

In Asia, there are a number of national conferences, such as Australian Conference on Information Security and privacy, Japan Security workshop and ChinaCrypto, etc..

In recent years, more and more researchers and technical people have joined on cryptography and security in Asia. It is said that in Asia, there are, at least, eight thousand more people professionally working on cryptography and information security.

The cipher and security mechanisms has been widely applied to industries and commercial areas in Asia. The governments and industries also provide more funding to academic institutes and the Universities. Industries began to set up their own cryptographic teams in Asia, such as NTT, Mitsubishi and Gemplus and DEC.

We wish that ciphers and security would go as fast as Europe and North

America.

Report on Canadian Crypto Policy Framework for Electronic Commerce
by Stewart Baker and Elizabeth Banker

The Canadian government released a discussion paper yesterday [Feb. 21, 1998 -eds.], "A Cryptography Policy Framework for Electronic Commerce," which evidences a surprising willingness to consider domestic regulation of use of encryption and a tightening of export controls. The report invites public comment on several options. The recommendations on export controls are of concern mainly to companies with Canadian-produced encryption products (especially software), and the recommendations on encryption of transient or communicated data will be of concern mainly to telecommunications companies and to companies acting as certification authorities in Canada. The options concerning possible mandated recovery of stored data could affect all encryption providers that sell products in Canada. (This is also the first opportunity offered by a Western government for public comment on the feasibility of mandated key recovery.)

Depending on the level of interest among our clients, we will likely file comments on at least one and possibly all of the three main policy areas covered by the notice. Comments are due April 21. If you would like to participate in the preparation of comments, please contact Stewart Baker by email (sbaker@steptoe.com) or phone (202-429-6413). More details about the options can be found below.

Canada, like many other countries, has been prompted to review its encryption policy both by the need for and growing use of strong encryption technology to support personal and business use of electronic communications, as well as the potential frustration of law enforcement and national security objectives resulting from use of such technology. Thus, the Task Force is reviewing Canada's current policy and seeking to update it. The new Canadian policy will also have to be aligned with the Wassenaar Arrangement, of which Canada is a member, and the OECD guidelines on cryptography.

The discussion paper proposes a series of options for stored data, real-time communications, and export controls.

Stored Data

The first option for encryption of stored data would involve no change to the current government policy and would allow market forces to dictate the data protection measures that companies and individuals would put in place. It would be up to individuals and businesses to decide whether to have back-up keys and where to store them.

The second option would mandate a minimum level of security and possibly explicitly require business data recovery. This option would involve government mandated standards for certification authorities and others offering key management services. The net result would be a government-sanctioned list of certification authorities offered to the public.

The third option would mandate use of key recovery products that allow law enforcement access to stored data with a court order. The government would prohibit the manufacture, use or import of non-key recovery products in Canada.

Real-Time Communications

Again, the first option presented would involve no change of the current policy. Telecommunications providers would continue to be obligated to assist law enforcement in intercepting and decrypting communications, to the extent able, when presented with a court order. However, decryption capabilities are not universal and most carriers are not required to maintain back-up copies of encryption keys.

The second option would require that all carriers that provide encryption service retain the capability to decrypt messages for law enforcement or national security agencies when presented with a court order.

The third option broadens the mandate of the second option to include the requirement that any certification authority providing a key for encrypting real-time communications make that key available when presented with a court order. Under this option, encryption products could not be used by individuals or by carriers that would not allow law enforcement access.

Export Controls

Relaxation of export controls is the first option presented. Relaxation could either be accomplished by adopting the most liberal export controls currently in use by another country or by considering foreign availability during license review.

The second option is to maintain the existing policy, including the exception for mass market products and public domain software. Under this option, Canada could continue to be neutral to key recovery products or allow foreign availability to be considered to give key recovery products some preferential treatment.

The third option would tighten export controls by eliminating the exceptions for mass market products and public domain software and by also only allowing export of strong encryption with key recovery features.

The final section of the paper invites comments on the options presented and poses several policy questions on how best to secure electronic commerce, balance individual privacy interests with law enforcement and national security concerns, and how to allocate costs of controls. The full text of the report is available at http://strategis.ic.gc.ca/SSG/cy00005e.html

---

New Federal Standard for handling sensitive data to take effect

---

Federal Information Processing Standard 140-1 stipulates requirements for the cryptographic processing of sensitive but unclassified data. This standard is due to become madatory June 30. Many hardware and software products have been designed and ceritified to be FIPS 140-1 compliant. However, there has been some resistance to implementation, especially within the Department of Defense. Primary complaints include the consumption of limited channel capacity, and the need to use Netscape and/or UNIX. Many DoD sites use a Microsoft environment for their Defense Message System communications. This makes it difficult for them to implement FIPS 140-1 because Microsoft products are not currently compliant. (This paragraph largely derived from an article in Government Computer News by Christopher J. Dorobek)

As reported in Cipher EI #20, February 10, 1997, FIPS 140-1 implementation requires that, after 31 January 1997, "only FIPS 140-1 validated cryptographic modules will be considered as meeting the provisions of this standard." Prior to this deadline, it was acceptable to purchase modules that had been submitted for evaluation, but had not yet been validated, or modules that had simply been claimed by their makers to conform to the standard. A list of such modules and more details on the requirements can be found at http://csrc.nist.gov/fips/fips1401.htm

The US National Institute of Standards and Technology and the Communications Security Establishment of the Government of Canada are sponsoring a conference, Assuring Cryptographic Security: The Development, Validation, and Use of FIPS 140-1 Compliant Products in Gaithersburg, MD USA May 11-12, 1998. Conference Web page is http://csrc.nist.gov/cryptval/

New National Information Protection Center announced,
FBI infrastructure intrusion detection program included

US Attorney General Janet Reno recently announce a new National Information Protection Center (NPIC). This will be an interagency center initially including personnel from the FBI, Secret Service, and Departments of Defense, Energy, and Transportation. Private sector companies are also expected to take a role. One element is a recent program by the FBI to allow real-time intrusion-detection. This is intended to help protect infrastructure elements such as the electrical power grid and telecommunications systems which are operated by the private sector. The plan is to allow digitally signed reports to be sent to an FBI server, which then anonymizes them and disseminates the information to other program participants.
(From reports in Federal Computer Week by Heather Harreld and Torsten Busse)

More recent news on Canadian Crypto Policy Framework
and other policy news

On March 31, 1998, leaders of Canada's cryptography industry and privacy
advocates met in Ottawa to discuss and suggest an encryption plan for
Canada. As always, crypto policy debate stirs up much opinion.
A story prompted by the meeting can be found in Wired News at
http://www.wired.com/news/news/politics/story/11397.html
Also, a press release on the topic was issued by Electronic Frontier
Canada, which can be found at the URL
http://insight.dcss.mcmaster.ca/org/efc/pages/pr/efc-pr.20apr98.html

The current (March '98) IFIP newsletter contains a proposed policy on
cryptography by TC11. The policy statement is prefaced by a statement
of the importance of cryptographic mechanisms in the Global Information
Infrastructure and an acknowledgement of the varied and sometimes
conflicting needs at play in determining crypto policy.
The whole issue of the newsletter is available at:
http://www.ifip.or.at/newsletters/nl1q98.htm

There was also a US Senate Judiciary subcommittee hearing on
encryption discussing primarily domestic controls on March 17.
Testimony of two who spoke can be found at
http://www.cdt.org/crypto
Also there can be found testimony by FBI director Louis Freeh
before the Senate Select Committee on Intelligence on January 28
concerning cryptographic based threats to US national security.

US congressional representatives Eshoo (D-California) and
Tauzin (R-Lousiana) have introduced the bill HR2991. Among other
things, this bill reguires federal agencies to make available
to the public forms that can be submitted electronically and
digitally signed.

The NSA has prepared a report presenting potential threats
to cryptographic systems when key-recovery has been employed.
The report simply details a number of potential attacks. But,
it is sure to affect the debate between encryption rights advocates
and proponents of key recovery, such as the FBI. A version of
the report, explicitly labelled ``not an official NSA document"
is available from Federal Computer Week. The report and related
stories can be found under the URL
http://www.idg.net/idg_frames/english/content.cgi?vc=story_8953.html

Also, see the references below to postings of a recent crypto
policy survey, and the reference above to the IEEE CS
survey currently being conducted.

Denial of service attacks targeting Windows 95/NT machines

This special edition of the CERT Summary reports denial of service attacks targeting a vulnerability in the Microsoft TCP/IP stack. We have received reports from a number of sites and incident response teams indicating that a large number of machines were affected.

The attacks involve sending a pair of malformed IP fragments which are reassembled into an invalid UDP datagram. The invalid UDP datagram causes the target machine to go into an unstable state. Once in an unstable state, the target machine either halts or crashes. We have received reports that some machines crashed with a blue screen while others rebooted.

Attack tools known by such names as NewTear, Bonk, and Boink have been previously used to exploit this vulnerability against individual hosts; however, in this instance, the attacker used a modified tool to automatically attack a large number of hosts.

The solution to protect Windows 95 and NT machines from this attack is to apply the appropriate Microsoft patch. The Microsoft patch, as well as more information about the vulnerability, can be found in the January 1998 Microsoft Market Bulletin entitled, "New Teardrop-like TCP/IP Denial of Service Program" available from:

http://www.microsoft.com/security/newtear2.htm

Although the first instance of this attack, which started March 2, 1998 appears to be over, keep in mind that the tools to launch this attack are now available and we expect to see more incidents of this type.

Network Associates buys TIS
Employees buy ORA Canada

Network Associates, Inc. and Trusted Information Systems, Inc. (TIS) announced on February 23rd that they have signed a definitive agreement where Network Associates will acquire TIS in a stock-for-stock pooling of interest merger valued at over $300 million. The full press release is available from TIS at the URL:
www.tis.com/corporate/press/98/nai-tis.html

On April 3rd, 1998, ORA Canada (Ottawa, Ontario) and Odyssey Research Associates (Ithaca, New York), closed an agreement in which an ORA Canada employee group acquired full control of ORA Canada. Terms of the agreement were not publicly disclosed. As of closing, ORA Canada becomes a Canadian Controlled Private Corporation.
Further information is available at the URL: www.ora.on.ca
or by email from dan@ora.on.ca

Frame relay outage causes disruption in AT&T network

Officials blamed a set of three unique circumstances for the April 13 failure, which kept thousands of transaction-oriented customers like banks and credit card centers off the network for between six and 26 hours, depending on the customer. First, said the officials, an upgrade procedure for firmware on a circuit card inside a Cisco switch was "inadequate," partly because it allowed maintenance while the switch was still connected to the network. There were no customers hooked up to the switch, the officials stressed, so the device was considered inactive.

Second, the officials said, a command in the procedure triggered software flaws on the circuit card being upgraded and the switch started to loop. In this condition it sent out to the other switches a surge of false signals that swamped the network and eventually brought it to a halt.

Third, software installed to monitor system health failed to recognize the signal storm as being false messages and so did not cut off the offending source. The reason, said the officials, is that administrative messages of the sort sent out in last week's failure often are sent out in great volumes, especially after a node has gone down and is being brought back online.

The combination of the three problems caused serious problems in the network and received national attention.

COMMENTARY AND OPINION

Web Security. A Step-by_step Reference Guide,
reviewed by Bob Bruen, Cipher Book Review Editor

Web Security. A Step-by_step Reference Guide. By Lincoln Stein.
Addison Wesley Longman, Inc. 1998. 436 pages. Bibliography and index.
29.95 ISBN 0-201-63489-9 LoC TK5105.59.S74

The author of "How to Set Up and Maintain a Web Site" has produced a wonderful companion to it with this new book. A very readable and practical work, it gives clear instructions to the reader on how, and why, to make a web site as secure as possible (although we all know that is a moving target). If you have not given much thought to securing your web site, this is a good place to start. If you have given it some thought, this book will serve as a checklist and will probably show you one or two items you may have missed. The World Wide Web Security FAQ, authored and maintained by Stein, was the basis for this guide, but it is goes well beyond the FAQ.

The book is organized into three main parts, (1) Document Confidentiality, (2) Client-Side Security and (3) Server-Side Security. Chapter one is a short introduction to web security. Chapter two, the usual introduction to cryptography, and chapter three, a good introduction to SSL (secure socket layer), SET (secure electronic transactions) and other digital payment systems make up Part 1. Part 2 contains chapters four, more on SSL, chapter 5, ActiveX, and chapter 6, web privacy. The ActiceX section is particularly worth reading if you are using it at your site. The design problems unique ActiveX are brought out so that anyone can understand them. This only uses up about 150 pages of the book, the bulk of the book is in Part 3. All of the chapters have resource lists (on-line and in print), as well as a handy checklist of the things you should have learned while reading the chapter.

Part 3 is composed of chapter seven through fourteen. The expected chapters on servers and security are present, but he has gone a step further to include Windows NT web servers, with all of the associated idiosyncrasies. He devotes a chapter to access controls and another to certificate based access controls, one of a number of places that SSL appears in the book. Stein takes the reader through the process of using certificates and even becoming your own certifying authority.

One of the best chapter is twelve, where CGI scripting is presented. No web site worth its salt can ignore this topic. He gives lots of excellent examples of code and improved approaches to common mistakes that leave the door open for the bad guys to come through. I especially like his explanations that really show the reader why something is a problem, not just a statement that it is a problem. He has achieved his goal making this book a practical tool that is actually useful. He seems to prefer Perl for his scripting language, providing a perl script to torture test your web server for some basic problems. He emphasizes logging of events and reading logs, one of those important but disliked, system administrator tasks.

The last two chapters cover higher level security management of a web site that can be easily overlooked. If you have more than a couple of people writing web pages for your site you run into problems of providing different levels of access, both on site and off site. There is a chapter on remote authoring and administration and the last chapter deals with firewalls and web sites, completing the package. He gives good advice on the appropriate approaches to handling web authors.

While no book covers everything, and certainly not in enough detail, this one does a fine job of covering base line security for your web site. I put this one right next to his "How to Set Up and Maintain a Web Site" on my book shelf, with a space for his next book. Stein is making valuable contributions to solutions for web security making him worth reading.

CONFERENCE REPORTS

Workshop on Education in Computer Security (WECS '98)
Pacific Grove California, USA, January 19-21 1998
by Cynthia Irvine.

The second Workshop on Education in Computer Security (WECS'98) was held from January 19 through January 21, 1998 at the Asilomar Conference Center in Pacific Grove, California. Sponsored by NPS CISR and DISA, the objective of the meeting was to permit security educators to share ideas and techniques for relating complex ideas in computer security to students. The theme of the 1998 meeting was effective use of the laboratory in computer security education. El Nino provided a window of beautiful weather. During breaks, participants strolled the beach and enjoyed the forest setting of one of the Monterey Peninsula's most scenic locations.

We had a pot luck: everyone brought a successful laboratory exercise to share. There was considerable diversity. Topics included network attack/defend; ethics and awareness; cryptography and protocols; passwords and viruses; systems; databases; intrusion detection; formal methods; and network security. In addition, to the variety of topics, the exercises spanned a range of prerequisite knowledge and sophistication, with some exercises for beginning undergraduates and others intended for advanced students.

The first day began with a session entilted Attack/Defend with the first talk by Lt Col Greg White (US Air Force Academy) who described the integration of security topics into a traditional computer science program and the use of laboratory activities to convey security topics. These included implementing a rudimentary cryptographic algorithm in an programming course, designing a virus to learn assembly language, and case studies in trusted operating systems. A capstone exercise involved Linux systems. Here students had to load the operating system, install security patches, and then attack the systems of their fellow students, while defending their own. Willis Marti (Texas A&M University) followed with a discussion of his network security class in which students learn about the defense of networks. What was surprising was the amount of time devoted to teaching ethics and the fact that it took almost three-quarters of the semester to prepare students to conduct an attack/defend exercise.

This led into the next set of presentations on ethics and awareness exercises. Aaron Enright (Wentworth Institute of Technology), a newcomer to computer security education described his plan for an exercise intended to change student perceptions of the players in the security arena. He noted that many undergraduates glorify hackers and consider security as "bad." When laboratory exercises make students the victims of hacking, they may have a better appreciation of defenders. During the discussion period, many agreed with Daniel Faigin when he suggested that system administrators should be depicted as the real "good guys" of the computer world.

Rich Plishka (University of Scranton) discussed the use of security labs in undergraduate computer literacy courses. In a series of simple exercises students learn that they do not work in completely secure environments, but that they must be vigilant. Nancy Mead (Software Engineering Institute) suggested role playing exercises to increase student awareness of a number of simple security measures that non-experts can easily take. These included: account borrowing, software piracy, and accidental virus propagation. It seemed to be an effective "ice-breaker" for a new class.

Following a break, we reconvened to hear about exercises on Cryptography and Protocols. The session started with John Hale (Washington State Univ.) who described a series of graded exercises in which students implemented cryptographic algorithms, cryptanalysis techniques, and protocols. Dan Zhou (Syracuse University) gave a presentation on the formal specification of protocols. Using pencil and paper rather than mechanical proof systems, students analyze properties of several protocols. A particularly interesting presentation was that of Enrique Daltabuit (Universidad Iberoamericana) and A. Gonzales (National Autonomous University of Mexico) who gave back-to-back talks on an exercise to develop secure electronic voting. One exercise focussed on the protocols and mechanism for casting ballots while the other pursued the design of a system for processing the ballots. They noted that since many students were first time voters and that they had participated in an important election, the topic of secure elections held the interest of the students.

Moving to another topic, Daniel Warren (Naval Postgraduate School) described an exercise to illustrate viruses. Because many of his students were not in computer science or engineering, he designed the exercise to use only the Bourne Shell. Using the "shell virus" he illustrated concepts including: access control, false positives, and false negatives. Jeff Bauer (Florida State Univ.) described an exercise for a beginning programming class in which students designed and implemented a simple password server. This was a project with a lot of benefits: not only were students given an introduction to passwords, but the also learned how to implement hash functions.

Following a wonderful Asilomar lunch -- lots of fresh vegetables, good home-style cooking and a view of the beach -- we moved on to Systems. Linda Wilkens (Bridgewater State College) presented exercises on protection that were used in a special topics course and included files, accounts, and e-mail. Each exercise began with a discussion and continued with activities to learn about and experiment with the protection of the item in question. The exercises seemed adaptable to new platforms and, with their use of the Web, easily modernized. Mark Hudson (U.S. Air Force Academy) followed with a presentation on exercises for an advanced course on Security and Information Warfare. Using a specified target system, students explored the use of various tools to learn how both administrators and hackers might use them. These included Crack, Satan, Courtney and Gabriel. As part of a course on secure systems Cynthia Irvine (Naval Postgraduate School) asked students to investigate the exploitation of the TS flag covert channel on Intel x86 processors. Students developed assembly language programs which they tested on a Linux system, where the channel worked, and on a Class B3 XTS-300, where the channel failed. The session concluded with a presentation by Ed Schneider (Institute for Defense Analyses) on the use of chat rooms to illustrate the concept of an information domain. It allowed students to explore policies for application-specific security contexts.

Each day, morning presentations were followed by working sessions in which participants subdivided into four groups to address a variety of topics. On the first afternoon we discussed the kinds of laboratory exercises appropriate to a survey course in computer security and their placement within the syllabus. The context of a course had to be determined in order to select appropriate exercises: the level of sophistication of the students in computer science, equipment resources available, whether students are on-site or remote, and, in the case of attack/defend exercises, various institutional and legal issues. In addition to the laboratory exercises brought to the meeting the groups suggested many new ones. In the area of protection, students could conduct a literature search on object protection, by examining the effects of viruses in Unix or PC systems they could learn about the protection of memory and addressing, they could design an access control mechanism, and they could implement a password policy enforcer to explore user authentication. While studying administrative security, they could use tools to identify and/or exploit security flaws as well as experiment with techniques to map policy into system configurations. To understand enterprise and organizational security problems, students could translate an organizational profile into a security policy. A simple risk assessment for a well-defined environment would give students experience in risk analysis. Similarly, by writing a security plan, students' classroom work would be reenforced. Exercises in disaster recovery could include analysis of log files, creation of a disaster recovery plan, and an exercise to bring the site of a simulated disaster back on line. Several suggestions were made for clever cryptographic exercises. For example, students could play roles in the writing and signing of an on-line will or other legal document. A simple hospital example could be used to demonstrate concepts of database and workflow security. It was suggested that movie clips could be used as a starting point for discussion: How was the alien ship attacked in "Independence Day?" Should there have been a notion of roles and least privilege for the systems in "Jurassic Park?" Could "Sneakers" really happen? One of the groups suggested that to demonstrate denial of service, the instructor, in collaboration with the system administrator, could slow down the response time of the system when students had a deadline. Of course, this would have to be exercised under controlled and limited conditions so that student stress levels would not become to high! A recurring theme was the need for realistic case studies. These ran the gamut from those describing the legal aspects of electronic commerce, to intrusion detection and disaster recovery, to examples of effectively designed systems.

A new addition to this year's meeting was a presentation giving the attendees an in depth look at a particular topic in computer security. During the second morning, Daniel Faigin, of the Aerospace Corporation, gave an excellent presentation on Penetration Testing. He discussed the differences between penetration testing and functional testing; gave a comparative description of the flaw hypothesis and attack tree methodologies; and gave the group guidance on planning a penetration test in a classroom setting. For those attending, Dan's tutorial provided framework in which to teach students about penetration without encouraging reckless behavior. Tutorials will be a part of future workshops.

Following another lunch overlooking the Pacific, we attended the session on networks. Jim Davis (Univ. of Iowa) presented a capstone exercise for a network security course in which students were tasked with obtaining a file from behind a firewall. They had to learn or find the network topology, file names, passwords, and encryption keys necessary to achieve this goal. Don Marks (NIST) discussed an exercise in which students used simple tools such as Perl scripts to detect intrusions in realistic datasets obtained from Dr. Georges Grinstein. He noted that it is often easier to detect anomalous behavior than to explain its cause. Fresh from graduate school Dr. Brenda Timmerman (California State University, Northridge) gave a presentation on using the problem of insuring e-mail privacy and traffic flow confidentiality as a vehicle for introducing exercises in formal methods, system environments, covert channels, system configuration, and evaluation and testing. Finishing the session was a demonstration of an exercise on SSH (Secure Shell) Derek Simmel (Software Engineering Institute). Derek brought laptops with him and showed us how the SSH exercise allowed students to learn how to successfully administer a system and install software that would provide protection against many of the vulnerabilities of the traditional "r-" commands. Not only did the exercise encourage good security habits, but it allowed students to creatively think through configuration decisions in a protected environment.

Workshop discussions on the second day centered on the problem of designing laboratory exercises with the equipment at hand. Several groups indicated that some simulations, perhaps written in Java, would be very useful for educators. A "national security playground" was suggested. Whether this is actually feasible, it is an intriguing idea: just as we have mega computer centers, a center for security experimentation could be established. (Don't sign me up to be a system administrator there!) A list of "essential" lab equipment was identified. It would have to be reconfigurable, flexible, inexpensive, and require low administrative overhead. The user machines could be x86-based systems with SCSI support and perhaps capable of booting multiple operating systems. One machine could be shared by two students. A locked-down server-class machine would be needed. It would be equipped with modems and a network printer. One or more network hubs and/or firewalls would complete the picture and would include, for example, an Internet gateway and be partitionable. Operating systems could be something from Microsoft and free Unix. Programming would be conducted in Perl, tcl, and C or C++. System analysis tools in the form of freeware would permit experiments to be designed.

The last set of workshop discussions dealt with describing minimum and ideal laboratory requirements and cooperation between institutions to create more realistic laboratory exercises. Everyone agreed that, in general, designing laboratory exercises was very challenging and, with the rapid developments in computer and network security, designing timely, pedagogically useful labs was quite difficult. Sharing of information was considered extremely helpful. Laboratory equipment can range from highly sophisticated and expensive to relatively simple. One group suggested that they would like the following: systems to illustrate discretionary access controls (Class C2) and those to enforce mandatory policies (Class B2), modems, logic analyzers, an encrypting router, lots of PCs, and groupware for projects. another group noted that just setting up laboratory exercises can be extremely difficult: qualified personnel are needed just to put systems back on line after the students have made a mistake or after an attack/defend exercises. Others suggested that corporate sponsors might be able to help, both with equipment and with case studies. These ideas merged well with those of another group, which suggested that experiments with VPNs might be interesting. Other aspects of emerging technologies to be formulated into exercises were comparisons of execution models for Web-based environments, experiments to provide authentication for downloaded executables, and virtual meetings. The suggestion was made that interesting cooperations could be created between computer science students and business students.

WECS'98 was very successful and each participant took home a package of laboratory exercises. The program committee consisting of Cynthia

Irvine, Daniel Warren, Daniel Warren, Deborah Frinke, Jim Davis, and Heather Hinton as well as the considerable help of Anastascia Cruz-Tokar contributed to an interesting workshop. A WECS mailing list has been set up by Rich Plishka. Write to: wecs-l@cs.uofs.edu. Participants expressed interest in exploring the use of tools and case studies in teaching computer and network security. These topics will help to set the theme for the WECS'99 which is being planned for early January 1999, once again at Asilomar.

Computers, Freedom and Privacy (CFP '98)
Austin Texas, USA, February 18-20 1998.
by Danielle Gallo.

Computers, Freedom and Privacy '98 was held February 18-20 at the Austin, Texas Hyatt Regency Hotel. Although there have been eight in total, this is the first CFP I attended. The program featured daily single-track sessions, lunch breakout sessions, and several concurrent tutorials.

I attended the Wednesday morning tutorial entitled, "An Introduction to Copyright and Trademark Law." This tutorial, given by David J. Loundy (http://www.Loundy.com) of Davis, Mannix and McGrath, was a comprehensive and enlightening overview of the workings of copyright and trademark law. An interesting question of public display was addressed. If an image is displayed on a Web page that does not belong to the owner of the image's copyright, are display rights violated? Using several case studies as examples, Loundy suggested that the answer depends on the type of browser being used. Is it a text-based browser that will not display the image? If an image is present but not displayed, is there a violation? If so, who is at fault, the Internet Service Provider or the Web designer? This tutorial also discussed trademark law, especially as it applies to metatags. Search engines use metatags to help index Web sties. For example, the playboyxxx.com site contains the keywords "playboy", "playmate", and "centerfold" in its metatags. However, this is deceptive because the surfer believes he is accessing a site supported by Playboy.

The remainder of the Wednesday session featured a keynote speech by Brian Kahin of the White House Office of Science and Technology Policy (http://www.whitehouse.gov/WH/EOP/OSTP/html/OSTP_Home-plain.html). Kahin addressed the future of Internet policy and discussed the effects on employment and productivity. He presented basic principles focusing on recognizing the unique qualities of the Internet and creating policy that will facilitate international commerce. One of Kahin's last points was the need for industry self-regulation. Kahin suggests that self-regulation creates more efficient markets. Kahin also cited the need for well-defined principles and international agreements as fundamental to success. International agreement appears to be a difficult process, as all parts of the world do not necessarily agree on major issues, such as privacy. Although Kahin strongly urged the private sector to lead such a movement, it seemed doubt surfaced among some attendees as to whether this is possible.

Anne Beeson of the ACLU, attorney Lance Rose, and UCLA school law professor Eugene Volokh discussed the Communications Decency Act decision. Volokh) argued that although the CDA was a victory for free speech, the decision should be examined with scrutiny. Volokh felt the CDA decision suffered from poor fact finding. Volokh's documentation regarding the Reno v. ACLU decision is worth accessing (http://www.law.ucla.edu/Faculty/volokh/index.htm). Ann Beeson (http://www.aclu.org) claimed that celebration for the CDA was significantly well justified. Beeson also stated that the architecture of the Internet promotes freedom of expression, and threats to this right lie in Senator McCain's bill, ratings/private censorship (including PICS), and library filtering. One interesting example Beeson cited was a student whose individual homepage was removed after people complained about it. As expected, this raised a strong reaction from the crowd.

A panel on 'Privacy Implications of Biometrics and Behavioral Identifiers' outlined the implications of the use of biometrics (thumbprints, retinal scans, etc) for identification purposes. Dr. Ann Cavoukian, the Ontario Information and Privacy Commissioner, presented the idea that biometrics are a threat to individual privacy when not used carefully. Dr. George Tomko of Mytec Technologies discussed combining biometrics with encryption in an effort to reduce privacy concerns and increase security.

The last panel for the Wednesday session addressed Net Vengeance. The "Kashpureff incident" was addressed and discussed in great detail. The basic conclusion was that significant collateral damage resulted from his offense; however, he accepted responsibility and offered regret. This was not the highlight of the panel. Richard MacKinnon of the University of Texas at Austin (http://bertie.la.utexas.edu/depts/gov/home.htm) sparked a discussion on the proper procedure when disciplining an offending online user. Since people from all nations participate in computer-mediated offenses, where and how should they be disciplined? The logical answer appears to be in their country of residence. MacKinnon suggests, though, that the offender may be judged by the standards of the group the offense occurred in. This apparently promotes preservation of the environment's integrity through punishment based on the environment and its members.

Wednesday closed with dinner and live music at the Austin Music Hall.

The Thursday general session began with a panel on 'Pragmatism and Principle in Online Advocacy." Danny Weitzner from the Center for Democracy and Technology (http://www.cdt.org) joined Donald Haines from the American Civil Liberties Union in a friendly discussion. Even though the panelists were supposed to be arguing different points of view there was much agreement. They agreed on the need for involvement in the political process but differed on what approach to take.

Although many ideas and issues were raised in the panel on 'Privacy and Encryption Law in France', there are only a few I would like to touch on. Professor Joel Reidenberg of the Fordham University School of Law (http://www.fordham.edu/law/faculty/reidenberg/main.htm) cited the territorial impact of data protection. He suggested trans-border data flows enable data passing to places with inferior protection. This is of utmost concern to the French, who hold strong views on privacy. The French position on data protection issues prevents sensitive data such as political or religious beliefs to be transmitted without consent. Reidenberg concedes that there is not full respect for data privacy laws; therefore, organizations have been created to supervise enforcement -- for example, the CNIL (Commission Nationale Informatique et Libertes) in France. This part of the discussion relates to Brian Kahin's keynote address, which cited the need for international agreements and well-defined principles. I think that compromise on these issues will be difficult because the French are very stringent on privacy issues and may not agree with the rest of the world.

The lunch breakout sessions offered a decent variety in subject topics.
I attended 'How to Do a Wiretap' with Shabbir J. Safdar from The Voters Telecommunications Watch. This was an entertaining session because the information was relayed in the form of a mock wiretap involving lawyers, government agents, and snowboarders. The snowboarders possessed illegal drugs and the FBI wanted to set up a wiretap to monitor their conversations. Safdar outlined the process of obtaining a wiretap, focusing on the necessary requirement, predicate offense, and probable cause. He also outlined minimization, which is the capture of material relevant to the investigation only. For example, the wiretap was shut off when the snowboarders began discussing the 'killer slopes, dude'. When the snowboarders began using snowboarding lingo as code words for drug lingo, the taping was resumed. Finally, a few interesting tidbits: computer fraud is not a valid predicate offense; 8 out of 10 offenses involve gambling and the Mafia; rules for data interception are less stringent when dealing with equipment such as pagers.

Matt Blaze and Steve Bellovin from AT&T Labs Research (http://www.research.att.com) discussed ways to 'Choke the Net.' Blaze and Bellovin cited the Net's structure as the cause of vulnerability.
In addition, the technical characteristics of HTTP are a mismatch with what the Internet was designed for. To choke the Net, certain computers such as endpoints or central routers can be brought down. The Net is not just susceptible to intended takedown, however. Circumstances such as real-time multimedia and high bandwidth data will disable the Net. Routing problems, specifically misconfigured routers, were cited as a final threat. I agree with the panelists' contention that protocols for secure DNS will decrease the risk of malicious attacks, though it is questionable by what fraction the risk will be decreased.

Thursday closed with a controversial panel on 'Crypto and Privacy at the Fringes of Society' moderated by Michael Froomkin from the University of Miami School of Law (http://www.law.miami.edu/). Patrick Ball of the AAAS Science and Human Rights Program (http://www.aaas.org) outlined security problems and provided crypto solutions for human rights organizations. He stated that human rights groups need encryption and digital signatures for protection. Ball finds traffic analysis a major threat to privacy, and suggests the use of anonymous remailers. Peter Toren from the United States Department of Justice (http://www.usdoj.gov) took the opposing view (big surprise there). Toren outlined the law enforcement perspective on crypto and privacy. He stated that unbreakable encryption will threaten public safety because it can be used to conceal criminal activity. He said, "advances in technology should serve society not rule it." Furthermore, Toren suggests that privacy and liberty must be protected without leaving a harbor for criminality. Toren's comments created strong response from the attendees and consequently, the question and answer session was lengthy.

In addition to the many thanks to Toren for actually attending, the Q & A featured predictable responses from each side. Matt Blaze expressed an interesting analogy in describing a paper shredder that created a digital copy of a document and sent it off to a central database. When a document was accidentally shred, the user could contact the database and have a copy faxed. Also, Toren was pressed about the encryption issue and repeatedly cited the significant increase in cases that involve unrecoverable evidence due to encryption. The government's case is made at http://www.fbi.gov/congress/encrypt/encrypt.htm . Audience members complained that the government repeatedly gives misleading information about the difficulty of cracking various encryption schemes.

Following the Thursday evening dinner reception and entertaining speech by Nicholas Johnson, there were a number of BoFs held. I attended the GILC (Global Internet Liberty Campaign) BoF. This informal discussion group featured Mark Rotenberg from GILC (http://www.gilc.org) and Barry Steinhardt, counsel to the EFF (Electronic Frontier Foundation, http://www.eff.org). Among other things, GILC has argued against PICS (Platform for Internet Content Selection). The BoF had a surprise element in the attendance of Paul Resnick, a professor at the University of Michigan School of Information (http://www.si.umich.edu/). Resnick is one of the developers of PICS. The discussion became a preview of the panel on the neutrality of technology and the question of 'is PICS the devil?'.

I did not attend the Friday morning session in its entirety, so I will glaze over these panels. 'Archiving the Web' was a rather uneventful session that discussed online archives and their implications for privacy and copyright. Among the services highlighted was Deja News (http://www.dejanews.com/), a USENET archive.

I attended the lunch breakout session on video surveillance, "Is Big Brother Watching You?" The answer is yes. Donald Haines of the ACLU addressed the rise in usage of surveillance equipment due to decreases in cost. An example is the ITS, or Intelligent Transportation System. The ITS is designed for traffic analysis and management, yet it is commonly used to facilitate the mass and routine surveillance of crowds. Another example is E-Z Pass, a toll collecting service used in New Jersey and New York. When a driver passes through the gate, his account number is scanned and posted on a screen. Haines suggests that any particular car can be monitored each day based on the account number scanned when the driver passes though. Time lapses between measurements can be used to observe the driver's speed and possibly result in a speeding ticket. Hashing the account number so it was not available at the second monitoring position would give the driver anonymity. Haines concluded with an emphatic need to increase the amount of privacy protection. He referred attendees to the Electronic Privacy Information Center (http://www.epic.org -- an interesting but unrelated paper on this site is (http://www.epic.org/Reports/surfer-appendix.html).

The Friday afternoon session featured a lively panel on library filtering. Susan Getgood was the first speaker; she is a representative for The Learning Company (http://www.cyberpatrol.com/), the makers of Cyber Patrol filtering software. Getgood stated that the makers of Cyber Patrol will not market to libraries but will definitely sell to them. I accept this point as the Learning Company is in a business that wants to make a profit along with helping children surf safely. I think, though, that if librarians are going to purchase the product they need to know what limits filtering has. Charles Harmon presented the opposing view and argued that filters are against the library's mission of providing access to information. Harmon said, "the use of filtering software to block sites is against ALA (American Library Association, http://www.ala.org) amendments." Harmon stated that NO software will ever meet the standard for libraries, and filters impose the producer's viewpoint on the community. For criticism of Cyber Patrol, see http://www.spectacle.org/cwp/ada-yoyo.html. Many attendees lined up to disagree with Susan Getgood during the question and answer period. One attendee raised a good point in stating that many library software users don't have a technical background, thus they are not fully aware of how to use software products. Library users need to be informed of how the technology works, its limitations, and how to use it successfully. Finally, I felt Susan Getgood did an admirable job defending her product despite the heated comments directed at her by libertarians. She stated that she believes Cyber Patrol is a product worth purchasing, and 68% of the parents in California who use technology to monitor their children's surfing agree with her. And no, they aren't going to publish the list of blocked sites.

Now, for the $64,000 question. Is PICS the devil? I dont think a definite answer surfaced. Panelists included Paul Resnick and Andrew Shapiro. Shaprio was highly opposed to PICS because it can be used to facilitate censorship. Resnick rebutted by stating that tools for censorship already existed before PICS. This question and answer period was also lively, including many comments directed at Resnick. Personally, I feel that PICS has provided a useful starting point and foundation for the selection of Internet content.

Bruce Sterling's "Thoughts on the Future" was an entertaining speech that contained a great deal of ranting. The part I found interesting was when Sterling addressed the Monica Lewinsky scandal. He stated that she poses no real threat to the country, is not a terrorist, and there is no need to observe her. Following the speech, Sterling hosted a party at his house for CFP attendees.

As a final note, I think that next year's conference should feature a panel on taxing electronic commerce. President Clinton endorsed no-new-Net-taxes legislation in his recent remarks to the Technology 98 Conference in San Francisco, but the future on this issue is unclear. Although this area does not relate directly to privacy or free speech, it is an interesting issue to examine within the realm of e-commerce.

*Random notes by the author: I liked the hotel but was disappointed to learn that the pool was outside. Could anyone tell me where to score a pair of John Gilmore's cool tie-dye socks? Bruce Sterling throws a good party. On Thursday, Richard Stallman explained that free software is like free speech and not free beer, but CFP seemed to do well in both departments. By Friday I felt like I had eaten my weight in tortillas. You're all checking out Crowds (http://www.research.att.com/projects/crowds/), right? Lastly, as this was my first visit to Texas, I was strongly encouraged by my cab driver to get a tattoo and eat a steak. I did not do either of these things, but enjoyed myself anyway.

Danielle M. Gallo (fmdk@nji.com) 03/01/98

Financial Cryptography (FC '98)
Anguilla, British West Indies, February 23-25 1998
by Paul Syverson.

The second annual Financial Cryptography Conference (FC98) was held in Anguilla in the British West Indies on February 23--26, 1998. The conference was a rousing success, Attendance was up with over 100 participants from business, academia, and government with interests in cryptology, computer security, and/or the financial industries. A governing body over the conference was introduced, the International Financial Cryptography Association, and held its first meeting, electing a board consisting of Vince Cate, Bob Hettinga, Ray Hirschfeld, Lucky Green, and Ron Rivest.

The presentations were interesting and well attended, no mean feat considering the Caribbean diversions that surrounded the participants. The quality was probably best summed up by David Chaum who remarked on the last day, ``I can't remember the last time I sat through an entire session much less a whole conference, but I came to every paper here."

The following description will focus on the official program. This means that it will deal almost entirely with presentations by cryptology and computer security researchers. Unlike last year, there were no papers presented by members of the financial community or policy experts. Those contributions occurred entirely in presentations and panels that were not part of the official program. This was unfortunate. Given the available distractions, these unofficial sessions were much less well attended. The ones I did attend were very instructive in understanding the financial side of financial cryptography. Had they been part of the official program, there might have been even more of a dialogue between the two sides that give the conference its name. Which is not to say that interaction was minimal, far from it. But the official dialogue was a bit one sided. (A much more off-program description of the conference can be found at http://www.live.co.uk/ftvfr398.htm)

The conference opened with welcoming remarks from the chairs and from Victor Banks, the finance minister of Anguilla. He noted that Anguilla was well suited as the site of the conference, observing that it may have more web pages per capita than anywhere else in the world. He also noted that revolutions, particularly bloodless revolutions, do well in Anguilla. And, like their own revolution in the late 1960s, he held high hopes for the revolution in electronic commerce at the forefront of which one can find this conference.

The first session began with a paper on ``Micropayments via Efficient Coin-Flipping" by Richard Lipton and Rafail Ostrovsky. The goal is to minimize communication: number of rounds, number of bits sent, hardware requirements, fraud, and computational requirements. In this scheme a coin-flip protocol is performed on the links of preprocessed hash chains formed independently at the vendor and the customer. Coin flips resulting from the chain results will only infrequently indicate a payment. The bank participates only when a payment is required. This is somewhat similar to Rivest's ``Electronic Lottery Tickets as Micropayments" which was presented at last year's rump session and was published in the final proceedings (which are now available from Springer). However, as Ostrovsky later explained at the rump session. the two are not the same. One difference is that, roughly speaking, Rivest's scheme backloads the winning result onto the lottery protocol, while the Lipton-Ostrovsky scheme frontloads the winning result.

The next paper was ``X-Cash: Executable Digital Cash" by Markus Jakobsson and Ari Juels. The basic idea is to have applets carrying cash that they can spend under appropriate conditions. The contribution of the paper was to show how to do this in such a way that the applet cannot easily be pickpocketed by an attacker or hostile host.

The first session ended with ``Distributed Trustees and Revocability: A Framework for Internet Payment" by David M'Raihi and David Pointcheval. One goal is to relax constraints on usual trust model and reduce trust assumptions of previous work. One may adopt different approaches to the use of trustees: trustee in every transaction, trustee just at account opening, or trustee only in anonymity-revocation. The paper combines the last two of these. It is based on the use of smartcards with user pseudonyms. The paper also makes use of a threshold approach to anonymity revocation so that honest users get assurance of privacy against a (small number of) compromised trustees.

David Maher presented ``A Platform for Privately Defined Currencies, Loyalty Credits, and Play Money". This was also a smartcard scheme. But, the idea is to have a fairly generic smartcard on which a number of different private currencies could easily be maintained. He sketched a number of potential applications: vendor loyalty points, corporate scrips, and monetary values for virtual environments like MUDS and interactive games. The idea is to have the currencies be easily defined and implemented as well as fungible with more ordinary currencies. It seems like a very interesting idea; although some in the audience questioned whether vendors would want to be bothered with the infrastructure overhead.

``Assessment of Threats for Smart Card Based Electronic Cash" was the next paper, by Kazuo J. Ezawa, Gregory Napiorkowski. It prompted lots of detailed questions. As was noted by Ron Rivest during questions, the threat model was someone trying to get money out of Mondex by counterfeiting cards rather than say a competitor trying to undermine confidence in the Mondex system. This was acknowledged as the focus of the work.

The last paper of the day was ``Using a High-Performance, Programmable Secure Coprocessor" by Sean W. Smith, Elaine R. Palmer, Steve Weingart The talk nicely outlined all the problems in developing building deploying, and updating (the software on) secure coprocessors.

Gene Tsudik kicked off the Tuesday program talking about ``Secure Group Barter: Multi-Party Fair Exchange with Semi-Trusted Neutral Parties", which he wrote with Matt Franklin. The Franklin-Tsudik approach uses unbalanced verifiable secret sharing to increase efficiency. They reduce all types of multiparty exchange to single unit cyclic exchange. In the multiparty case, principals will get what they want. But, principals may not know from whom they get it. Cyclic order is hidden by the STNP, and it does not necessarily know the size of the group.

The next paper was ``A Payment Scheme Using Vouchers" by Ernest Foo and Colin Boyd. The voucher approach uses the same payment principals as other approaches: the customer, the bank, and the merchant. The main difference is that it reverses the usual payment cycle.

-bank and merchant create a voucher
-merchant sends the voucher to customer (including encrypted goods)
-customer sends voucher with cash to the bank
-bank evaluates voucher
-bank informs merchant and
-bank releases voucher to customer
Vouchers are made only when merchant wants to make a new product Then they sit on the ftp site and wait for customers. Efficiency was claimed over, e.g., Netbill and iKP Also, there is no online processing by merchant. Like Netbill, goods are part of the protocol, not just cash is sent. One can have customer anonymity via anonymous ftp, but not anonymity from the bank. Detailed comparison was given of the number of messages, symmetric encryptions, the location of computation, signatures, etc. It was noted that this scheme is not as efficient as some of the micropayment schemes. Also, it goes against the usual network thinking by placing load at the bank. But, it requires less work by the merchant. A question was raised about static vs. dynamic products This scheme only allows static (predetermined) products.

The next paper was ``A Formal Specification of Requirements for Payment Transactions in the SET Protocol" by Catherine Meadows and Paul Syverson. SET is the proposed industry standard for credit card transactions on the Internet. This paper gave an overview of the payment part of SET. Requirements were given in NPATRL (the NRL Protocol Analyzer Temporal Requirements Language) for analysis using the NRL Protocol Analyzer. Modifications and additions to NPATRL needed to formalize requirements for SET were also described.

Markus Jakobsson presented a position paper written with Moti Yung entitled ``On Assurance Structures for WWW Commerce". The motivating question was, ``What is left to do to facilitate trade over the Internet?" The current environment was claimed to be characterized by lawlessness, changing identities, and gang wars, where one must be careful carrying cash, and there are no road signs. Basically, they compared the World Wide Web with the wild and wooly west. (Within this the western theme Markus described the good, the bad, and the ugly of what is on the Web.) Main components of the infrastructure needed are the access structure, for people to find the goods and services they need, the trust structure to facilitate trust between customers and merchants. Also needed are protections in other contexts. Anonymity, freedom from profiling, prevention of access to information, and [forced access to information] i.e., direct marketing, were all raised. Basically the need for both individual and institutional rights. Finally they noted the need for a means for maintaining the structure of assurances. They also considered the economic, legal, and other impediments to providing these needs.

The next program elements was a panel discussion on the Mechanics and Meaning of Certificate Revocation moderated by Barb Fox(BF). Other panelists were Joan Feigenbaum(JF), Paul Kocher(PK), Michael Myers(MM), and Ron Rivest(RR).

BF began by characterizing revocation as the undoing of a persistent signed statement. The reasons could be either key compromise or some sort of relationship binding failure, either a key to an identity or an identity to a CA (certification authority).

Questions for panel given were: Can X.509 work? What are the alternative CRLs? And, what about revocation across PKIs? Other questions were: Who owns a certificate? Who pays for revocation? What is the relationship between revocation and trust management? Finally, should we wait for legal mechanisms?

MM noted that we can't solve all the problems today, but major corporations want to use this today to manage their risk. There is also nonrepudiation and other issues besides risk management. He noted that a CRL can be good for many needs even if it is just a blacklist, and CRLs are well position in architectures today. But, on the other side he noted their large size and inability of the basic approach to handle timeliness effectively. The alternative of short lived certificates take advantage of existing mechanisms and are easy to deploy within an enterprise. But, the don't scale well; it must be decided for how long they are valid. Thus, it is somewhat a case of just moving the bandwidth elsewhere. He also mentioned pros and cons of on-line and off-line approaches.

PK claimed that revocation is needed to make public key crypto automatic. Solutions must consider security, scalability, performance, memory (smartcards), bandwidth, auditability, practicality wrt what is currently available, secure manageability, and simplicity (e.g., should use standard crypto).
CRLs fail at least wrt reliability, scale, performance, memory, bandwidth,

and practicality (applications don't know where to get CRLs from). Valicert's approach is to use Certificate Revocation Trees and he claimed that these meet all the requirements.

RR gave his position as one favoring no certificate revocation. Certificates support a signed message/request. Freshness matters to acceptor (more than the CA), so freshness requirements must be set by the acceptor not the CA. Corollary: periodically issued CRLs are wrong. E.g., a badge checker wants at most day old badge information but CRLs come out once a week.
He then gave the SDSI model in which the signer must get the freshness evidence, not overworked server. And, the simplest freshness check is a (more) recently issued certificate. He noted that key compromise is different. Who controls a key's good/compromised bit? He noted that the PGP suicide note is no good in the case a where a key is deliberately shared. He proposed a network of suicide bureaus with which you register when obtaining a public key. Suicide notes can be sent to any suicide bureau from which it will quickly be disseminated to all. This means that you can obtain a health certificate from the bureau with which you registered saying that you indeed are registered and no evidence of problems with your key has been received. He ended with a bit of advice from the grammar and style classic by Shrunk and White: always go positive when you can.

JF said that she agreed with everything Ron said especially, put it in positive terms. She noted that the cost of infrastructure maintenance is crucial. Fast cross PKI checks will be expensive, but probably can be minimized.

After basic positions were given the panelists all generally agreed on things ;>). For example, Matt Blaze (one of JF's co-creators of Policymaker) asked, ``Is it worth it to build this whole infrastructure to have certificate revocation?" MM responded that there isn't much infrastructure difference between revocation and validation. To which JF responded, ``No. There's a big difference."

David Aucmith pointed out that devices (not people) often carry keys. And, they can't make suicide decisions. For them CRLs are important. This was one question for which I didn't hear a good answer to, although something akin to Rivest's suicide bureaus might also be able to handle this.

Presumably if evidence of compromise has arisen somewhere, then the device will not be able to obtain a certificate of health when needed. It's inability to function should then ultimately attract the attention of a human who can then decide to obtain a new key for the device.

Someone else raised that CRLs are a mechanism for managing changing trust, but why should we think that this one mechanism can handle all the trust management available from public keys? If there is evidence that my key was compromised two weeks ago, I can incorporate that in a CRL, but how could you do this on the positive approach? It can't go back in time like a CRL can. Ron Rivest said that this was a tough problem and he didn't know the answer. But he added, "that's what juries are for."

After dinner Tuesday night was the first meeting of the International Financial Cryptography Association (IFCA). As mentioned above, a governing board was elected. The other main topic of business was where to hold future conferences. After much animated discussion it was decided that the conference would stay in Anguilla for at least the near term.

Following this, there was a rump session.

John Kelsey described cryptanalysis of the SPEED Cipher (work done with with Wagner, Hall, and Schneier). The SPEED cipher was introduced at FC97 by Yuliang Zheng. He observed that the interesting part was the cryptanalysis that fails. The obvious differential attack doesn't work. Instead they use a related key attack.

Ian Grigg announced NISI Advanced Encryption Standard Support They will do the JAVA implementation for any algorithm that anyone wants because NIST wants 3 implementations for standards including one in JAVA. They're the middle men. They need volunteers to do it.

Stephan Overbeek described the N-count value Analyzer. It is based on one-way chaining in smart cards. Value is in the number of chain links revealed (reversed). The claimed main difference is that the 1-way chain is specific to a terminal rather than the user. It was claimed to be fast and good for micropayments.

Cathy Meadows gave a quick overview of the NRL Protocol Analyzer,
an interactive Prolog based tool for analyzing cryptographic protocols.
It examines a protocols by starting in a final state and searching
backwards to see if it is possible to reach an insecure initial state.
It is thus like a model checker. But unlike a model checker, it sometimes
analyzes infinite state spaces, which it does by facilitating the proving
of lemmas (like a theorem prover) that allow pruning of infinite chunks
off the search space.

Alain Mayer described policy issues for running an anonymizing service.
He raised three general problems that might arise, not necessarily
specific to Lucent's LPWA.
-Your service is used for a(n attempted) break-in at another site.
-somebody posts threats or insults on a message board via your service.
-a site asks you to block access from your service to the site.
I noted that all three of these had actually occurred with our Onion
Routing prototype, and that at the time we were struggling with general
policy solutions to these problems. (We have since formulated a policy,
which is posted on our Web site. LPWA has also posted a policy statement
at http://lpwa.com:8000/policy.html)

Rafi Ostrovsky explained why Rivest's Lottery scheme is not equal to
the Lipton-Ostrovsky given on Monday. The difference has been described
above in the synopsis of his Monday presentation.

Paul Syverson presented Weakly Secret Bit Commitment. I gave an example
of an exchange protocol with no trusted third party where the
principals are not forced to be fair but rather where their incentive
to proceed outweighs their incentive to cheat.

Jon Ziegler described the Java Ring, which is Java running on a Dallas
semiconductor iButton. Amongst other nifty features, it does garbage
collection so you can delete applets when their done.

David Goldschlag presented Security Models for content. This was an
overview of the Divx approach to, e.g., ``renting'' movies, in which
the rental period starts when the movie is first played rather than
when it is obtained and there is no need to return the DVD. To allow
you to `re-rent' the disc the DVD player has a dialup connection to a
backend system. The DVD player logs the disc serial number of played
discs and reports the log periodically to the backend (offline). If

you prevent the player from calling in for a long time it will lock up. Questions were raised about privacy. David responded that release of a customer profile is better protected than at conventional video rental chains where the cashier has your profile rather than an access protected billing service.

Stuart Stubblebine presented On Revocation. This was roughly improved or extended versions of Rivest's principles (given during panel, c.f., above). The principles were related to his own work on recent security and metrics of authentication. One example, Rivest principle: Freshness requirements must be set by acceptor not a CA. This was amended to: Freshness requirements must be set by all entities relying on them.

Bob Green described what it was like to be a Programmer Living in Anguilla. This wasn't really on the topic of the conference. But, it gave a fascinating glimpse of what it is like to work in Anguilla. Some advice and comments gleaned from the talk. If you want to move here, bring two of everything that can break. Officially on paper, you can't move, so you just do it. If you fix somebody's PC there, you now know their whole family. And, since there are only a handful or so of families on the island, you get to know everybody pretty quickly.

Bob Hettinga presented Market model for bearer certificates. He suggested that we should base it on the old physical bearer bond model. Major Claim: even if you issue a bearer certificate at every exchange, that's still cheaper than, e.g., seven years of credit card audit trails.

Steve Schear rounded out the evening with a description of First E-Cache.

Wednesday morning began with an invited talk by David Chaum, who I think could reasonably be called the undisputed father of financial cryptography. The title of his talk in the preproceedings was ``Private Signatures and E-commerce''; however, the title on his opening slide was ``Which Flavor Will Win in the `Way-More-Digital' World''. This brief writeup can only sketch some of the many topics on which he touched.

There were two foci to his talk, info technology policy issues and privacy, particularly in payments.

His policy overview covered three areas. (1) commons issues: free bandwidth has had a positive effect on cyberspace growth (2) consumer protection: false privacy? (3) human rights: next wave of fundamental human rights is informational rights. Consumer protection and bandwidth intersect at junk mail and push technology. Consumer protection and human rights intersect at the consumer platform and interface. And, bandwidth and human rights intersect in the area of message encryption secrecy. In the intersection of all three is access -- interaction security (people have to be able to protect their interests in cyberspace). He went on to describe both the problems and facilitating factors of establishing interaction security.

He began his discussion of privacy by noting: The consensus of the heads of major technology companies, Greenspan, others is that consumer confidence in privacy protection is the major reason that e-commerce hasn't taken off. In fact, surveys even show that people are generally expecting increased privacy from e-commerce vs. current commerce. He then explained some of the drawbacks of e-commerce using conventional payment mechanisms such as credit cards and explained how blind signatures enable one-way private e-cash. He felt it was quite important to stress that it is one-way privacy not anonymity, as is often said in the media. In other words, nobody can without your agreement know where you spent your money BUT, you can always prove with the bank's help who received any payment, as well as when and for how much.

His conclusion was that there were forces moving us in two directions.
flavor #1: an all traceable nonrepudiable more-centralized world, and
flavor #2: an expanding decentralized informational-rights world
(the good one). He didn't say definitively which way things would go, but he felt that work such as done by the attendees of this conference would help push in the right direction.

A fascinating claim that he made during questions, but on which he did not have time to elaborate was that, with the various cryptographic and other mechanisms he had described in his talk, the possibility exists to virtually eliminate of organized crime.

The conference continued with ``Group Blind Digital Signatures: A Scalable Solution to Electronic Cash" by Anna Lysyanskaya and Zulfikar

Ramzan, who split the presentation duties. Their model is of a central
bank with smaller banks that users choose. The goal is to make the
Goal: identity of the user and of the user's bank anonymous to the
vendor and the vendor's bank (only the central bank can find out the
issuing bank of a piece of e-cash. And, no bank (even central) can
issue cash in another bank's name. The scheme is online, hence somewhat
expensive. But it can be made offline if we compromise a degree of
user anonymity.

Before the next session Ian Goldberg announced that he had a 100 byte program
to turn an export version of Netscape into one with all the strong
crypto and announce a contest to write a smaller one. He also extended
the contest to write a similar program for Internet Explorer.

The next talk was ``Curbing Junk E-Mail via Secure Classification'' by
Eran Gabber, Markus Jakobsson, Yossi Matias, and Alain Mayer (the last
of whom gave the talk). H e noted that spamming is currently easy:
it's easy to to gets lots of addresses and to send to them, and it's
hard to distinguish spam from other mail. There are tools available,
but their solution was claimed to have advantages over each of them.
The gist of their solution is to have extended email addresses,
basically you have a core address plus extensions for use with
multiple groups of users. A handshake to the core address just gets
extensions This deters spammers and adds functionality. Also, you can
later revoke an extension (by filtering all messages with that
extension). So a spammer buying the address from another spammer won't
get any value since the extension is revoked. This approach is claimed
to be provide transparency of extensions to actual users, robustness
(flexible about how much automation is used) backwards compatibility
with sendmail, etc., and -interoperability with the rest of the world.

Next up was ``Publicly Verifiable Lotteries: Applications of Delaying
Functions'' by David Goldschlag and Stuart Stubblebine. Regular
lotteries require trusting the auditors and determining the winner is
not repeatable since it relies on a random element. The goal here is to
find a fair, closed, and publicly verifiable lottery in which not
even the lottery agent is trusted. The basic idea is to make the
winning number calculation slow and require at least one random entry.
Besides the obvious application of running a lottery other applications
include distributed random numbers (with a low overhead of communication).
It was also shown how to use delaying functions in the exchange protocol

I described in the rump session.

The next paper was ``Security of Digital Watermarks" by Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, and Francis X. Zane. This was a very nice survey of existing watermarking technologies. Their stated goal is to have invisible and robust watermarking: only the key holder can find it, and it can't be removed without destroying the data. The focus was on perceptual content (video, etc.) rather than representational content (programming text, etc.) It was noted that it may be Important to have layers of marking for e.g. private and public watermarks.

After lunch came ``Security in the Java Electronic Commerce Framework" by Surya Koneru, Ted Goldstein. The talk was given by John Ziegler. The talk contrasted commerce with EDI. Commerce is not about absolute trust. In fact, spontaneous commerce requires zero trust in the principals; all trust is in the payment token. The opposite extreme is EDI, where trust is in the long term relationship, and the payment token can be just about anything. Their offerings are Java Commerce Beans and Java Commerce Client (a wallet). Java Commerce Client anchors the client side of the transaction, handles client delivery, installation, update, cooperation with a trusted and familiar interface. Java Commerce Beans provide a structure for creating customer relationships: operations, instruments, protocols, services, etc.

Next up was ``Beyond Identity: Warranty-Based Digital Signature Transactions" by Yair Frankel, David Kravitz, Charles Montgomery, and Moti Yung. A standard CA architecture assures static properties, liability with respect to contract enforcement, nonrepudiation of signers, etc. The main concept of a warranty is that it addresses the need to further validate current contextual information beyond identity. A warranty granting transaction system is dynamic: providing warrants on a per-transaction basis, accounting for user history and providing user-specified access to control parameters.

The next presentation was ``Compliance Checking in the PolicyMaker Trust Management System" by Matt Blaze, Joan Feigenbaum, and Martin Strauss. The motivating problem for this presentation was: Even if wary customer Alice has convinced herself that Bob of small company Bobsoft signed a program so what? She wants to know if Bob complies

with her policy for buying software. The topic of this paper is: What
do we mean by proof of compliance? Compliance checking approach works
by incremental proofs using supplied credentials (authorizations). For
example, Cred1 is run and it says Bankofficer1 will approve if he sees
evidence of freshness. Cred2 is run and says fresh, Cred1 is run again
and says approved. Yes means there is some finite sequence of the
running of credentials there is an acceptance record that says the
policy is satisfied. But this is undecidable! (Various restrictions
can get this down to NP hard, or NP complete.) Nonetheless, this has
been implemented and runs in application. Applications noted as
described elsewhere include signed email, PICS labels, and license
management. Note that since policies must be monotonic you can't
directly do certificate revocation type things.

Next was ``An Efficient Fair Off-Line Electronic Cash System with
Extensions to Checks and Wallets with Observers" by Aymeric de Solages
and Jacque Traore. This paper is at the most recent in a chain of
papers making various improvements on Brands's CRYPTO 93 paper of
similar name. The present contribution is to improve the efficiency of
the payment protocol.

The final paper of the official program was ``An Efficient Untraceable
Electronic Money System Based on Partially Blind Signatures of the
Discrete Logarithm Problem" by Shingo Miyazaki and Kouichi Sakurai.
Those who stayed until this last paper were rewarded with an
interesting talk that began with a presentation of nondigital (hence
exportable) origami ninja weapons. The basic idea is that the signer
signs a blind part (user ID and coin number) and a clear part (validity
and amount of money). Partially blind signature makes the system more
efficient because bill amounts need not be tied to signing key, i.e.,
you don't need a separate key for $10 bills, $20 bills, etc. The
combined embedding and engraving signature scheme is designed to cover
all the types of information needed.

Thursday was primarily occupied by an empirical investigation of
so-called ``ecliptic curve cryptography". That is, most of us took a
boat down to a few miles off the coast of Montserrat to observe a total
eclipse of the sun while simultaneously keeping one eye on the volcano
spewing tons of ash just to our west. The geek-o-meter registered quite
high as several preprogrammed GPS devices could be heard going off when
the boat reached the contracted observation location. (Other evidence

of geekhood such as people spotted brandishing a laptop and a notebook on the boat and actually doing work are vehemently denied by this author.)

Friday after breakfast there was an unscheduled question and answer hour with David Chaum, which I was unfortunately unable to attend. After this there was a roundtable discussion on ``Financial Intermediaries, Public Networks, and Financial Cryptography" moderated by Steve Schear. Other presenters were Paul Guthrie, A.S. von Bernhardi (aka Black Unicorn), and Frank Trotter.

Steve Schear lead off with an overview. On a national level, the central bank is the ultimate financial intermediary---setting interest rates, rules for interbank loans, etc. Below them are the commercial banks. These do the financial networks and management for individuals and businesses. Below them are the credit cards between the banks and the consumers. These do risk management. There are also a large number of processors like First Data, and Virtual that sit between the bank and the merchant, as well as ATM networks like Cirrus and smaller regional associations like Most. Finally, there are also nonbank financial intermediaries brokers, check cashing services, etc.

Paul Guthrie gave a description of where things are going with card associations, which are made of member banks (Visa, Mastercard), and card companies, which have as customers rather the end consumer (American Express, Discover). For card associations, acceptance will imply certificates (making sure that the card is accepted at a store need merchant certificates since anyone can stick up a logo on a Web page). Cards will carry more software. There will need to be PKI infrastructures. There may be adoption of new payment systems. There will also be more opportunity for new brands in cyberspace. Thus, the meaning of brands must be made clearer. Adam Shostack asked: networks can be more open and yet there is going to be more certification of who is authorized to accept a card? Answer: It's up to the member bank, which merchants they want to back. More liberal banks will run a higher discount rate.

Frank Trotter began by observing that there are no hard currencies anymore and discussed the roles of some of the traditional players in the new world. He observed that state banks and regulatory agencies have increasingly less reason for being, resulting in various turf squabbles.
Banks meanwhile are trying to defend their current franchise value.

Banks provide credit stability for the consumer.
If anybody who sets up a private mint and goes bankrupt, that will kill the
the confidence in the market for some time.

At that point von Bernhardi brought up the story of the failure of the EU Bank in Antigua. This was basically an offshore, online bank that was destroyed and lost (only!) 12 million dollars. Someone noted that it's good this happened earlier when the sacrifice was small and everyone can make sure it doesn't happen again. The important danger is that institutional risk becomes systemic risk. Guthrie noted that Visa will drop banks that become a risk or will require a cash deposit in a third party neutral bank. Then, von Bernhardi contrasted public vs. private insurance (what he called ``the myth of government backing of financial institutions"). Trotter then pointed out that many other industries are are moving into banking. Telecom is the biggest threat to banking: they have a big base and good records. They could start to take deposits and get backing of FDIC.

In beginning his own presentation, von Bernhardi stated that, ``It's ironic I'm here... At the far end of the tunnel, I would like to see intermediaries diminish." He proceeded to give his impression as an offshore banker. The motivation is not to provide stability of the international financial community but to make money. Local offshore governments typically take an attitude of `if you behave here, you can stay'. The threshold of acceptable behavior is much higher than in the US. Regulators in the US are interested in providing global stability. Offshore banks MUST operate out of band, because they're there. To connect to the system, they have to go through the ACH (Automated Clearing House). They have to go through VISA. But, there's a lot more freedom. He would like to see financial intermediaries functioning in the exception rather than ordinarily in transactions. Consumer efficiency involves reducing the middle man. But, then how do we broker trust? Well you can have TTPs in the short run. Crypto protocols won't do the whole job. Offshore could use these new technologies so that they can go through these intermediaries faster. But, in the long run, fewer and more offline intermediaries is the way to go. Reputation, he noted, is a multifaceted issue. It's not just a question of having a certificate on the wall. ``If one of my clients walked in to Citibank with a cashier's check from us, I can guarantee that it won't clear right away."

Someone asked from the floor what will happen when we start to see private minting. etc. Bernhardi responded that selling your frequent flyer miles is now possible and becoming easier. And, Trotter observed that you build a trading system, and if enough trust is built into the system it becomes another currency. Someone else in the audience observed that the very existence of these systems is evidence of inefficiencies in the main systems. They will then adapt and primarily the small systems will remain small.

NSA Network Security Framework Forum (NSFF)
Baltmore Maryland, USA, March 2 1998
by Jeremy Epstein.

NSA Network Security Framework Forum (NSFF) Meeting Notes
Jeremy Epstein, Trusted Information Systems (jepstein@tis.com)

The NSFF (http://nsff.xservices.com) is a working group established by NSA to discuss DoD security needs. It meets about once every six weeks at the Maritime Institute near Baltimore MD. The following is a synopsis of one such workshop on MLS held 2 March 1998 in Baltimore. The meeting consisted of three main parts: MLS Past (a history of MLS), MLS Present (what's going on today), and MLS Future (what we should expect), plus an introductory session, a lunchtime session on their framework, and a wrapup Q&A session. There were about 250-300 attendees. For the number of words spoken, there were amazingly few interesting things said. The one sentence summary is that nothing is new in the wonderful world of MLS: some people think we still need it, other people thing guards do the job just fine, and there are very few new ideas on how to solve the problems that MLS was designed to address.

This report consists of two parts: the few interesting points and a summary of the sessions. The opinions are those of the author, and not necessarily those of his employer!

INTERESTING POINTS

Among the more interesting points in the meeting were:
* Some people are still arguing for MLS operating systems (e.g., Jim Anderson).
* While most vendors were represented, there were no representatives from

Microsoft there.
* At a recent high level meeting Microsoft was asked (by government representatives) about their plans for MLS, and was told that Microsoft has no interest in MLS.
* For the forseeable future, there's no real alternative to guards, even though they're admittedly dangerous.
* The hacker community (specifically, Phrack) has copies of the attack scripts used against the Pentagon in February, and is trying to decide whether to post them on their web site. (This was hallway chatter, not a presentation.)

SESSION SUMMARY

Session 0: Welcome, etc.

Dave Luddy (NSA X1) talked about the first public draft of "DoD Technical Framework for User/Applications-Layer Security Services" (formerly known as "Technical Framework for DoD Security Enabled Desktops") which is now available on their web site; and they are seeking industry feedback. The goal of the framework is to provide guidance on what's available today, as well as to guide industry on what NSA thinks is needed for tomorrow. The next NSFF meeting (April 16 & 17) is to discuss feedback on the framework. [As this article was going to press, that date has been cancelled. The workshop will be rescheduled for the summer.]

Session 1: MLS Past

Summary: We have the same MLS problems we've always had, and government has done a lousy job solving them.

Grant Wagner (NSA, session chair) reviewed what MLS is, and what the environment was (mostly large non-networked systems that were too expensive to afford one per classification). He then explained the attempted simplification of the yellow book (risk indexes) and how they tried to make it mandatory, with the goal of stimulating market demand. NSA tried to push vendors to build MLS products, but it failed miserably. The reasons for that failure included vendors and customers not believing in the threats (since NSA kept the good stuff classified), the lack of rewards to industry (government promised to buy MLS systems, but didn t in sufficient numbers to pay back the vendor investment), and customers were more interested in features than in security. Perhaps the most important reasons, though, are that (1) systems became too complicated for any real assurance and (2) the time to market overcame everything else in the product development processes. What we should do is return to original goals, by getting vendors and customers to sign on. The need is greater than ever: we have real attackers, mobile/malicious code, and risk management is harder than ever.

David Bell (Mitretek) also talked about what went wrong. We didn t leverage what we knew into new products and development. We set our goals too low: C2 by 92 set a minimum (which we missed) instead of trying for MLS. As a result, we overspecialized and overspecified:"we needed MLS, but got C2 and hi/low guards. DoD was caught off guard by pervasive networking, desktop advances, etc. The needs today are the same as before: MLS controls wherever there's data.

Marv Schaefer (Arca systems) talked about the changes in our computing environment. Systems went from monolithic computing to distributed, from configuration management to self-installing, self-extracting programs (10 years ago, we didn t have programs that installed themselves and unknown other software when you insert a CD into your PC), from professional system administrators to user self-administration (who are less skilled and less interested in security), from Trojan horses to applets and macros as the threats, and from skilled penetrators to hackers (who are less skilled, but better tools). The needs haven t changed though: we need a "sound balance of technologies and assurances: not a band-aid, never a tourniquet".

Jim Anderson (independent consultant) noted that "the traditional Bell LaPadula MLS model was right, it still is, and it met all its objectives". What went wrong is that the PC revolution caused evaluations to take longer than product cycles, the Government market didn't materialize, so vendors stopped investing, NSA didn't practice what it preached (no worked examples, no showcases, and demos were unrealistic), we ignored networks until it was too late, and we didn t pay attention to running COTS software at workstations. His chief point is that we haven t learned our lessons. Instead, we substituted "crypto is the answer, what was the question?", and substituted guards which are fundamentally wrong. The net result is that we lost capability: there are very few capable of doing MLS work any more. The INFOSEC community is proceeding as if MLS is a solved problem, but it's not. What we should do is build MLS products that run arbitrary COTS at workstation. The government will have to pay for MLS products, as no vendor would build on speculation after the government history of not purchasing the last generation of MLS products.

Session 2: MLS Present

Summary: People are using guards, and (IMHO) ignoring assurance.

Col Joe Sheldon (NSA, Chair) summarized the currently available guard solutions available including the C2 Guard, Ops/Intel workstation, N-level workstation, SNS Standard Mail Guard, ISSE Guard, Radiant Mercury, and MLS networks using SCO CMWs. Man-in-the-loop downgrade is common. The strategy for making COTS applications work on CMWs is to give them all the privileges, then remove them one at a time until the application breaks, and decide whether you can live with the risk of assigning the required privileges. (IMHO, this is a truly amazing approach to security.) NSA is working on building a version of the C2G that will pass MS Office documents from high to low. (It absolutely floored me that anyone would consider such a thing, given the amount of data hidden (i.e., object reuse problems) in MS Office files.) Auditing is a problem for all of the guards: too much data, too hard to analyze.

According to Col Sheldon, there are 539 MLS connections (e.g., Unclassified to Secret) fielded throughout DoD today! They re revisiting each of the accreditations now, and anything that isn't re-approved must be turned off in September. They have major data classification cascading problems, which aren't being addressed. He concluded by noting that technology isn't a panacea but procedures can help, and the guard product aren't perfect, but they're a solution.

Joe Alexander (Sun) noted that DoD isn't buying Trusted Solaris (which is one of the few commercial MLS products), but that other countries are, including UK, Canada, South Africa, Japan, Singapore, Poland, and Czechoslovakia. He noted with scorn that Australia has been buying Trusted Solaris, but decided NT was good enough. NCSC evaluations are important, but the ease of getting waivers make them irrelevant. At Sun, they have enough resources to evaluate OR develop new versions of the MLS product, but not enough sales to justify both, so they focus on building products and skip the evaluations. He concluded by noting that the "Internet is our greatest friend", because it s scaring people into buying security.

Capt Dan Galik (SPAWAR) described the IT21 program (Information Technology for 21st Century) which is putting PowerPoint and similar stuff on every desktop. He said that Microsoft told DoD they don't see any business case for MLS, so we shouldn t expect anything in that area (DoD is less than 1% of Microsoft s business, so even if DoD used MLS exclusively, it wouldn t be enough for Microsoft to spend their effort on it). As a result, IT21 is using multiple single level networks rather than MLS. In places where MLS is truly necessary, they are using a bunch of CMWs and some guards.

Erika Langerman (Joint Staff) is using SNS with SMART (Standard Mail Attachment Review Tool) to send email across levels. They re now sending 1500-2000 pieces of email per day from high to low, half of which have attachments. For moving data up, they re still using sneakernet. Since they re not doing MLS at the desktop, so everything is system high. They re also using "Cybershield" (which is the equivalent of the B2-targeted Dockmaster 2) to allow Top Secret users to go web surfing.

Louanna Notargiacomo (Trusted Computer Systems) described the Ops/Intel workstation, which is built on B1/CMW-like products from Sun & DEC. There are over 100 Ops/Intel systems fielded and accredited by DIA. For $3500, TCS will offer a Sun Ultra 5 that runs MS Office apps at multiple levels simultaneously. They also provide a MLS web server, and Trusted Oracle as the MLS DBMS. The SSL Proxy Gateway includes HTTP request filtering based on a dirty word search, and can also filter out executable content. The bottom line is that people just want to interconnect, so they do it without understanding the risks.

John Pescatore (TIS) got a good laugh with the comment that "any vendor who can't develop a product faster than government evaluates it is either (a) out of business or (b) a government contractor". He also commented that system high model is easier than MLS for all the standard reasons: competition vs. single vendor lock-in, understandable vs. hidden costs, expensive vs. really expensive, etc.

Lunchtime Session: User/Applications Level Security Services Framework

Todd Inskeep (NSA) described the framework, noting that it took the challenge from presidential commission to improve assurance. Their goal is to provide quick directions, and long term buyin. They want to rely on information security solutions from industry. The framework has three pieces: security services API, generic applications, and custom applications. The security services API includes security & crypto features for security aware applications (e.g., CDS, Microsoft crypto API).

The generic applications layer includes high assurance email with DMS, file encryption, databases, collaboration. (No explanation of how to justify the claim of "high assurance".) And the custom applications layer relies on using CORBA or DCE. They also want to address remote access. The framework draft (available on the web page) has been provided to big vendors (e.g., Oracle, Microsoft) for comments. A follow-up workshop on April 16 & 17 will review industry comments on the framework, with final release in June.

Session 3: MLS Futures

Summary: No one has any good answers for how to do things better.

Bill Neugent (MITRE) gave a very entertaining speech, with nuggets like: "If you like the features, who cares about assurance; if you don't like the features, who cares about assurance?" and "MLS: A good idea carried too far, or a bad idea carried too far?". He noted that NT 5.0 has 26 million lines of code, with an average of 20% replaced every year (we don't need no stinkin' minimal TCB!). Bill suggested that guards don't necessarily need high assurance operating systems for bases, as the security is at the applications level. He noted that we hear what the CINCs need, but not what we need for infrastructure protection. Buying MLS workstations isn t a solution, as they typically get put in the corner to gather dust. MLS protection needs intrusion detection systems that look at MLS-specific attacks, and shut off connections in case of attack. He suggested getting luminaries like Cheswick & Bellovin to look at how guards work and making suggestions for improvements.

Bill suggested some things we need to improve security, including tools that look for backdoors around guards and for illegal traffic, and low-side "detonation chambers" to try running attachments before sending them along to high systems. There should be many fewer interconnection points: not the 539 talked about by Joe Sheldon. Switched workstations are a great choice. We need to avoid overconfidence and stupidity (which is difficult, since we're not sure what it is that constitutes stupidity). He concluded by noting that we have to find solutions: "winning the war trumps saving the systems, unless losing the systems means losing the war".

Carl Landwehr (NRL) talked about a three simple technologies that can be used in place of building MLS systems: the NRL Pump sends information reliably from low to high; the Australian-developed Starlight provides safe

MLS windowing; and onion routing provides anonymous web browsing. We still need a downgrader, but given these tools there should be far less to downgrade. What we really need is more good ideas like these, rather than guards and similar devices.

George Schou (Oracle) talked about the increasing concerns about security in the commercial world. The commercial world is mainly interested in electronic commerce. He mentioned an NIH project (PCASSO, thePatient Centered Access to Secure Systems Online) which is the first civilian use of MLS.

Doug Schultz (USACOM) talked about the MLS hexagon: labelling standards, software for release, electronic tagging, personal authentication, MLS workstations, and MLS security. I didn't understand the point of his talk or what it *really* has to do with MLS.

Charlie Testa (Infosystems Technology) described Trusted Rubix, which is a DBMS hosted on a B3 operating system (XTS-300). It can be used to bridge Secret & SCI, with appropriate information flow enforced. Charlie claimed it can be used as a guard, although he didn t explain how it s a guard. ITI recently submitted RUBIX for NSA evaluation as a TNI/TDI "M" layered component on top of a Wang XTS-300. (IMHO, this is the same old MLS DBMS that no one wanted before, and I don t know why anyone would want it now.)

Last Session: Q&A/Wrapup
[Nothing reported]

Assessment of security software

UNIX security professionals, interested in attack and intrusion detection, are being invited to test and assess a new public domain combination of sensor and traffic analysis software. Deadline is May 1 for the assessment -- results will be distributed at SANS98 in Monterey. The goal is a joint effort to create a "cops for networks."

For an invitation to participate, email sans@clark.net with the subject "CID Information". Or go directly to the content at
<http://www.nswc.navy.mil/ISSEC/CID/cid_1_0.doc>
Sponsors: The SANS Institute and the Naval Surfave Warfare Center.

New Reports available via FTP and WWW

o http://www.secnet.com/papers/ids-html
Paper on intrusion detection systems and their weaknesses from Secure Networks, Inc.

o http://zdtv.zdnet.com/zdtv/Site/StoryFrameSet/0,1163,210,00.html
Feature article about encryption policy based on a
survey funded by the Soros foundation and conducted by EPIC.
URL for the survey follows.

o http://www.gilc.org/crypto/crypto-survey.html
A survey of International cryptography policy.
Detailed information can be found at
http://www.gilc.org/crypto/crypto-results.html

New Interesting Links on the Web

o http://www.Loundy.com/CDLB/
Technology Columns from the Chicago Daily Law Bulletin
Recent articles include
April 9, 1998: Junk e-mailers face attack on several fronts.
New legislation (Washington State), new court cases,
and new technology for addressing junk e-mail.
March 12, 1998: Filtering software poses legal pitfalls.
A discussion of filtering software in light of newly proposed
legislation and the Mainstream Loudoun v. Board of Trustees of
the Loudoun County Public Library.

Who's Where: recent address changes

Entered 18 February 1998

James W. Gray, III
RSA Data Security
100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031

(650) 595-7703 (voice)
(650) 595-4126 (fax)
jgray@rsa.com

Calls for Papers (full list on Web)

CONFERENCES

Listed earliest deadline first. See also Cipher Calendar.
Mix of full and abbreviated listings this issue; web will be updated
as soon as possible to include abbreviated listings.

HASE '98
http://kel7.eecs.uic.edu/hase98/
3rd IEEE High-Assurance Systems Engineering Symposium, November 13-14 1998, Washington DC. The objective of this Symposium is to provide an effective forum for original scientific and engineering advances in High-Assurance Systems design, development and deployment, and to foster communication among researchers and practitioners working in all aspects of high assurance systems. The Symposium Proceedings will be published by the IEEE Computer Society Press after the symposium meeting. The primary focus of the Symposium is on innovative research results in the area of high-assurance (highly reliable, highly available, safety-critical, real-time, and secure) systems. Complex systems' engineering issues, including hardware design, software engineering (both formal and informal methods), performance evaluation, and system assessment are particular focus of the Symposium. Of special interests are the integrated system design principles that consider multiple aspects of high assurance systems. The purpose of this Symposium is for public dissemination of such research results from academia, industry, and government. Paper submissions due 5/15/98. Panel submissions due 6/15/98. More submission information available from the Program Chair, Prof. Jeffrey J.P. Tsai at tsai@eecs.uic.edu or on the Web page.

ACSAC`98
http://www.acsac.org
Fourteenth Annual Computer Security Applications Conference, December 7-11 1998, Phoenix AZ. The conference solicits papers, panels, vendor presentations, and tutorials that address practical approaches to solving these problems in federal, state and local governments,

departments of defense, and commercial environments. Selected papers
will be those that present examples of in-place or attempted solutions
to real problems, lessons learned, original research analyses, and
approaches to securing our information infrastructure. All papers,
panel/forum proposals, and vendor and tutorial proposals are due by
May 29, 1998. Authors will be notified of acceptance by August 7,
1998. Camera-ready copies are due not later than September 25, 1998.
You can also contact Vince Reed at Publicity@acsac.org

RBAC '98
Third ACM Workshop on Role-Based Access Control, George Mason University,
Fairfax, Virginia, USA, October 22-23, 1998 (Submissions Due: May 15, 1998)
The ACM workshop on Role-Based Access Control (RBAC) brings together
researchers, developers, and practitioners to discuss the application
of RBAC to both traditional and emerging systems and the development
of new modeling paradigms. The workshop invites participation from
the database, network, distributed systems, operating system, security
and application communities. Users, developers and researchers are
invited to submit seven copies of their papers (in English and limited
to 6000 words) to the Program Chair at the address given below before
the due date (no electronic submissions will be accepted).
Outstanding papers will be considered for publication in ACMs new
Transactions on Information and Systems Security (TISSEC). Proposals
for panels and group discussions should be sent, preferably by email,
to the Panels Chair, David Ferraiolo, at dferraiolo@nist.gov.
Proceedings of the workshop will be published by ACM and will be
distributed at the workshop. Submissions should be sent to: Trent
Jaeger, IBM T. J. Watson Research Center, 30 Saw Mill River Road,
Hawthorne, NY 10532

JOURNALS
Special Issues of Journals and Handbooks: listed earliest deadline first.

o A special issue of IEEE Internet Computing on
Internet Security in the Age of Mobile Code, November/December 1998
Guest editors: Gary McGraw (gem@rstcorp.com) Edward W. Felten
(felten@cs.princeton.edu) Submissions are due May 12, 1998
URL for submission process information: http://computer.org/internet/
This special issue will be devoted to security implications of mobile
code. In particular, we are interested in articles discussing:
* Code signing technologies, including models for permissions,

capabilities, and principals

* Proof-carrying code and security policy resolution
* Implications of existing protocols such as SSL on proxy scanning, intrusion detection, and firewalling
* Handling denial of service
* Design of secure interfaces for devices such as smart cards
* Security policy creation and management issues
* Injecting security into the software development process

o A special issue of Software Practice & Experience on
Experiences with Computer and Network Security
Submission due: July 1, 1998
Guest editor: Gene Spafford
Papers describing both `systems' and `applications' software in any computing environment are acceptable. Typical topics include software design and implementation, case studies, studies describing the evolution of software systems, critical appraisals of systems, and the practical aspects of software engineering. Theoretical discussions can be included, but should illuminate the practical aspects of the work, or indicate directions that might lead to better practical systems. This special issue is specifically devoted to issues of computer and network security software. We are seeking high-quality articles relating to the above-mentioned themes. This includes papers on at least the following topics:

* access control systems
* auditing systems and analysis
* misuse and instrusion detection systems
* applications of cryptography
* secure messaging systems
* information protection systems
* security of mobile code
* security of browsers and related technology
* security testing and assurance
* firewall construction and testing
* experiences with new security programming paradigms
* development and experience with "hacking tools"
* experiences with patching security flaws

o A special issue of The Journal of Computer Security on
Research in Intrusion Detection.
Submissions due: July 15, 1998.

Guest editor: Phil Porras, porras@csl.sri.com.
URL for further information: http://www.csl.sri.com/jcs-ids-call.html
This special issue seeks papers that describe research beyond the scope or orthogonal to what the commercial intrusion-detection community is producing. The intent is to capture results from key efforts in the field, and to understand the directions and motivations that are driving current and future research in this area. Papers are solicited on all aspects of intrusion detection, including the extension of intrusion-detection techniques to new problem domains, as well as the application of other techniques to intrusion detection. Suggested topics include, but are not limited to

- Active response capabilities and cooperative decision support
- Cooperation policies and distributed correlation across administrative domains
- Cross pollination of intrusion-detection techniques and applications with other disciplines
- Formalization of activity modeling
- Integration into large scale environments, including efficient methods for high-volume event analysis
- Integration of intrusion-detection capabilities into existing network services, infrastructure, and management frameworks
- Interoperability and reusability among intrusion-detection modules
- Service-oriented intrusion-detection architectures (including work toward supportive services such as intrusion-detection management, dynamic registration, event collection, results interpretation)

Reader's Guide to Current Technical Literature in Security and Privacy
Part 1: Conference Papers

FC'98 - Financial Cryptography '98, Second International Conference, February 23-25, 1998, Anguilla, BWI. [Report of conference by Paul Syverson also given above. -eds.]
Conference URL http://www.cwi.nl/conferences/FC98

o Micropayments via Efficient Coin-Flipping. R. Lipton and R. Ostrovsky
o X-Cash: Executable Digital Cash. M. Jakobsson and A. Juels
o Distributed Trustees and Revokability: A Framework for Internet Payment. D. M'Raihi and D. Pointcheval
o A Platform for Privately Defined Currencies, Loyalty Credits, and

Play Money. D. Maher
- o Assessment of Threats for Smart Card Based Electronic Cash.
  K. Ezawa and G. Napiorkowski
- o Using a High-Performance, Programmable Secure Coprocessor
  S. Smith, E. Palmer, and S. Weingart
- o Secure Group Barter: Multi-Party Fair Exchange with Semi-Trusted
  Neutral Parties. M. Franklin and G. Tsudik
- o A Payment Scheme Using Vouchers. E. Foo and C. Boyd
- o A Formal Specification of Requirements for Payment Transactions
  in the SET Protocol. C. Meadows and P. Syverson
- o On Assurance Structures for WWW Commerce. M. Jakobsson and M. Yung
- o Group Blind Digital Signatures: A Scalable Solution to Electronic
  Cash. A. Lysyanskaya and Z. Ramzan
- o Curbing Junk E-Mail via Secure Classification.
  E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer
- o Publicly Verifiable Lotteries: Applications of Delaying Functions.
  D. Goldschlag and S. Stubblebine
- o Security of Digital Watermarks.
  L. Matheson, S. Mitchell, T. Shamoon, R. Tarjan, and F. Zane
- o Security in the Java Electronic Commerce Framework.
  S. Koneru and T. Goldstein
- o Beyond Identity: Warranty-Based Digital Signature Transactions.
  Y. Frankel, D. Kravitz, C. Montgomery, and M. Yung
- o Compliance Checking in the PolicyMaker Trust Management System.
  M. Blaze, J. Feigenbaum, and M. Strauss
- o An Efficient Fair Off-Line Electronic Cash System with Extensions to
  Checks and Wallets with Observers. A. de Solages and J. Traore
- o An Efficient Untraceable Electronic Money System Based on
  Partially Blind Signatures of the Discrete Logarithm Problem.
  S. Miyazaki and K. Sakurai

NDSS'98 - The Internet Society's Network and Distributed System Security
Symposium, San Diego, California March 11-13, 1998, USA.
Conference URL http://www.isoc.org/ndss98

- o Enabling the Internet White Pages Service - The Directory Guardian.
  D. Chadwick and A. Young
- o The Multilayer Firewall. D. Nessett and P. Humenn
- o Efficient Protocols for Signing Routing Messages. K. Zhang
- o Attack Detection Methods for All-Optical Networks.
  M. Medard, D. Marquis and S. Chinn.

o Distributed Algorithms for Attack Localization in All-Optical Networks.
R. Bergman, M. Medard and S. Chan.
o Credential Management and Secure Single Login for SPKM. D. H|hnlein
o Some Timestamping Protocol Failures. M. Just
o The Secure Remote Password Protocol. T. Wu
o On the Problem of Trust in Mobile Agent Systems.
U. Wilhelm, S. Staamann and L. Buttyan
o Implementing Protection Domains in the Java Development Kit 1.2.
L. Gong and R. Schemers
o Live Traffic Analysis of TCP/IP Gateways. P. Porras and A. Valdes
o Automated Recovery in a Secure Bootstrap Process.
W. Arbaugh, A. Keromytis, D. Farber and J. Smith

Second International Workshop on Information Hiding, Portland Oregon,
April 14-17, 1998, USA.
Conference URL http://www.cl.cam.ac.uk/~fapp2/ihw98

o Information Hiding to Foil the Casual Counterfeiter. D. Gruhl and W. Bender
o Fingerprinting Digital Circuits on Programmable Hardware.
J. Lach, W. Mangione-Smith, and M. Potkonjak
o Steganography in a Video Conferencing System. A. Westfield and G. Wolf
o Reliable Blind Information Hiding For Images.
L. Marvel, C. Boncelet, and Charles Retter
o Cerebral Cryptography.
S. Hou, Y. Desmedt and J.-J. Quisquater
o The Steganographic File System.
R. Anderson, R. Needham, and A. Shamir
o Stop-and-Go MIXes Providing Probabilistic Security In An Open System.
D. Kesdogan and J. Egner.
o Biometric yet Privacy Protecting Person Authentication. G. Bleumer
o On Software Protection Via Function Hiding. T. Sander and C. Tschudin
o Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations.
M. Kuhn and R. Anderson
o On Digital Watermarks. J. Fridrich
o Intellectual Property Protection Systems and Digital Watermarking.
J. Lacey, S. Quackenbush, A. Reibman, J. Snyder
o Copyright Techniques for Digital Images Based On Asymmetric
Cryptographic Techniques.
A. Herrigel, H. Petersen, J. Ruanaidh, T. Pun, and P. Shelby
o Throwing More Light on Image Watermarks. J. Hernandez and F. Perez-Gonzalez
o Continuous Steganographic Data Transmission Using Uncompressed Audio.

Chr. Neubauer, J. Herre, and K. Brandenburg
o Attacks on Copyright Marking Systems.
F. Petitcolas, R. Anderson, and M. Kuhn
o Testing Digital Watermark Resistance To Destruction.
S. Sowers and A. Youssef
o Analysis of the Sensitivity Attack Against Electronic Watermarks in
Images. J.-P. Linnartz and M. van Dijk
o Steganalysis of Images Created Using Current Steganography
Software. N. Johnson and S. Jajodia
o Twin Peaks: The Histogram Attack on Fixed Depth Image Watermarks. M. Maes

---

Reader's Guide to Current Technical Literature in Security and Privacy
Part 2: Journal and Newsletter Articles, Book Chapters
by Anish Mathuria

Computer Networks and ISDN Systems, Vol. 29, No. 15 (November 1997):
o C. Dalton and J. Griffin. Applying military grade security to the
Internet. pp. 1799-1808.
o D. Steves, C. Edmondson-Yurkana and M. Gouda.
Properties of secure transaction protocols. pp. 1809-1821.
o B.-J. Koops. Crypto regulations in Europe. Some key trends and issues.
pp. 1823-1831.

Computer Communications, Vol. 20, No. 14 (December 1997):
o W.-B. Lee and C.-C. Chang. Three ID-based information security
functions. pp. 1301-1307.

Computer Communications, Vol. 20, No. 15 (December 1997):
o W. Godoy Jr. and D. Pereira Jr. A proposal of a cryptography
algorithm with techniques of error correction. pp. 1374-1380.
o C.-H. Lin. Dynamic key management schemes for access control in a
hierarchy. pp. 1381-1385.

Computers & Security, Vol. 17, No. 1 (1998):
o Vesselin Bontchev. Macro virus identification proglems. pp. 69-90.

Information Processing Letters, Vol. 65, No. 1 (January 1998):
o P. Ryan and S. Schneider. An attack on a recursive authentication
protocol. A cautionary tale. pp. 7-10.

o R. Molva and G. Tsudik. Secret sets and their applications. pp. 47-55.

Information Processing Letters, Vol. 65, No. 2 (January 1998):
o G. Horng. An active attack on protocols for server-aided RSA signature computation. pp. 71-73.

IEEE Transactions on Communications, Vol. 46, No. 1 (January 1998):
o X. Lin, Y. Xing and Y. Yang. Comment on "Reparable Key Distribution Protocols for Internet Environments". pp. 20-21.
o T. Hwang. Author's reply. pp. 22.

IEEE Spectrum, Vol. 35, No. 2 (February 1998):
o S. Lodin and C. Schuba. Firewalls fend off invasions from the net. pp. 26-34.

IEEE Communications Magazine, Vol. 36, No. 2 (February 1998):
o J. Francis, H. Herbrig and N. Jefferies. Secure provision of UMTS services over diverse access networks. pp. 128-136.

Information and Computation, Vol. 140, No. 2 (February 1998):
o S. Low and N. Maxemchuk. A Collusion Problem and Its Solutions. pp. 158-182.

Communications of the ACM, Vol. 41, No. 3 (March 1998):
o H. Wang, M. Lee and C. Wang. Consumer Privacy Concerns about Internet Marketing. pp. 63-70.
o R. Hall. How to Avoid Unwanted Email. pp. 88-95.

IEEE Transactions on Communications, Vol. 46, No. 3 (March 1998):
o S. Low, N. Maxemchuk and A. Lapone. Document Identification for Copyright Protection Using Centriod Detection. pp. 372-383.

IEEE Communications Magazine, Vol. 36, No. 3 (March 1998):
o S. Burgett, E. Kock and J. Zhao. Copyright Labeling of Digitized Image Data. pp. 94-100.

IEEE Internet Computing, Vol. 2, No. 2 (March/April 1998):
o Y.-K. Hsu and S. Seymour.
An Internet Security Framework Based on Short-Lived Certificates.

IEEE Computer, Vol. 31, No. 4 (April 1998):

o M. Kang, A. Moore and I. Moskowitz. Design and Assurance Strategy
for the NRL Pump. pp. 56-63.

____

Calendar

____

==

See Calls for Papers section for details on many of these listings.

==

"CWP" indicates there is a hyperlink to a coference web page on the
Cipher Web pages. (In many cases there is such a link even though
mention is not made of it here, to save space.)

```
Dates         Event, Location    Point of Contact/ more information
-----        ---------------    ---------------------------------


 5/ 3/98- 5/ 6/98: IEEE-S&P; Oakland, California
 5/ 5/98- 5/ 7/98: DOCSec '98, Baltimore, MD
 5/12/98: Internet Computing, Mobile Code Sec. spec.iss. due gem@rstcorp.com,CWP
 5/29/98: 14th ACSAC; submissions due, contact Publicity@acsac.org, CWP
 5/31/98- 6/ 4/98: EUROCRYPT '98, Helsinki, Finland, CWP
 6/ 1/98- 6/ 5/98: 10th CITSS, Ottawa; citss@cse-cst.gc.ca
 6/ 1/98- 6/ 4/98: SIGMOD-PODS. Seattle, Washington, CWP
 6/ 8/98- 6/12/98: CAiSE*98, Pisa, Italy, CWP
 6/ 9/98- 6/11/98: CSFW 11; Rockport, Massachusetts, CWP
 6/15/98: RAID '98, Belgium, submissions due to raid98@zurich.ibm.com
 6/16/98- 6/18/98: NCISSE; Harrisonburg, VA; www.infosec.jmu.edu/conference
 6/17/98- 6/19/98: WETICE '98, Stanford University, California, CWP
 6/25/98: WFMSP, Indianapolis, Indiana, CWP
 6/30/98- 7/ 2/98: ISCC '98. Athens, Greece, CWP
 7/ 1/98- 7/ 4/98: SICON '98. National University of Singapore, CWP
 7/ 1/98- 7/ 3/98: Euro-PDS98. Vienna, Austria
 7/13/98- 7/15/98: ACISP '98, Brisbane, Australia, CWP
 7/15/98- 7/17/98: IFIP WG11.3, Chalkidiki, Greece, CWP
 8/10/98:  SETA '98, Singapore; Submissions to dingcs@iscs.nus.edu.sg
 8/17/98- 8/21/98: COMPSAC '98, Vienna, Austria
 8/24/98- 8/27/98: VLDB '98, New York City, NY, CWP
 8/24/98- 8/28/98: DEXA-WBPR '98, Vienna, Austria
 8/24/98- 8/28/98: NBIS '98; Vienna, Austria, CWP
 8/24/98- 8/28/98: MDDS '98. Vienna, Austria, CWP
 8/24/98- 8/28/98: ECOMM; Vienna, Austria, CWP
```

8/26/98- 8/28/98: DEXA-SIDIA '98, Vienna, Austria, CWP
8/31/98- 9/ 3/99: EC '98, Boston Mass., CWP
8/31/98- 9/ 4/98: IFIP/SEC '98, Vienna and Budapest, CWP
9/14/98- 9/15/98: RAID '98, Louvain-la-Neuve, Belgium, CWP
9/14/98- 9/16/98: ECC '98, Waterloo Ontario, Canada, ecc98@math.uwaterloo.ca
9/16/98- 9/18/98: ESORICS '98, Neuve, Belgium, CWP
9/21/98- 9/25/98: HPN '98, Vienna Austria, www.ikn.tuwien.ac.at/IKN/events/
9/22/98- 9/25/98: NSPW `98 Charlottesville VA, USA, CWP
10/ 2/98: IRW-FMP '98. Australia, CWP
10/ 5/98-10/ 9/98: NISS '98, Arlington VA, USA, http://csrc.nist.gov/nissc/
10/ 5/98-10/ 9/98: FMLDO 7, Ostfriesland, Germany, CWP
11/ 3/98-11/ 5/98: CCS-5. San Francisco, CA, USA, CWP
11/19/98-11/20/98: IIIS, Fairfax, VA, CWP
12/ 7/98- 12/11/98: 14th ACSAC, Phoenix, AZ, CWP
12/14/98-12/17/98: SETA '98, Singapore, CWP
1/ 5/99- 1/ 8/99: ECT track of HICSS-32, Maui, Hawaii
http://www.di.uoa.gr/~hicss32/e-commerce.html
5/ 2/99- 5/ 5/99: IEEE S&P 99; Oakland no e-mail address available
5/11/99- 5/14/99: 11th CITSS, Ottawa; no e-mail address available
8/23/99- 8/26/99: USENIX Sec '99, Washington DC, conference@usenix.org
4/30/00- 5/ 3/00: IEEE S&P 00; Oakland no e-mail address available
5/16/00- 5/19/00: 12th CITSS, Ottawa; no e-mail address available

Key:

* ACISP = Australasian Conference on Information Security and Privacy
* ACSAC = Annual Computer Security Applications Conference
* CAiSE*98 = Conference on Advanced Information Systems Engineering
* CCS = ACM Conference on Computer and Communications Security
* CCSS = Annual Canadian Computer Security Symposium (see CITSS)
* CITSS = Canadian Information Technology Security Symposium
* CFP = Conference on Computers, Freedom, and Privacy
* COMPSAC = Int'l. Computer Software and Applications Conference
* CRYPTO = IACR Annual CRYPTO Conference
* CSFW = Computer Security Foundations Workshop CSFW 11
* DCCA = Dependable Computing for Critical Applications
* DEXA = International Conference and Workshop on Database and Expert Systems Applications
* DEXA-SIDIA = DEXA Workshop on Security and Integrity of Data Intensive Applications
* DEXA-WBPR = International Workshop on Business Process Reengineering and

Supporting Technologies for Electronic Commerce
* DOCSec = Second Workshop on Distributed Object Computing Security
* EC = USENIX Workshop on Electronic Commerce
* ECC = Workshop on Elliptic Curve Cryptography
* ECOMM = Business Process Reegineering and Supporting Technologies for
  Electronic Commerce
* ECT = Electronic Commerce Technologies Track of HICSS-32
* ECDLP = Workshop on the Elliptic Curve Discrete Logarithm Problem ECDLP
* ESORICS = European Symposium on Research in Computer Security
* EUROCRYPT = IACR Annual CRYPTO workshop in Europe
* FSE = Fast Software Encryption Workshop
* HASE = High-Assurance Systems Engineering Workshop
* HICSS-32 = 32nd Hawaii International Conference on System Sciences
* HPN = IFIP Conference on High Performance Networking
* IEEE S&P = IEEE Symposium on Security and Privacy
* IFIP/SEC = International Conference on Information Security (IFIP TC11)
  IFIP/SEC '98 (Twelfth Annual)
* IFIP WG11.3 = IFIP WG11.3 11th Working Conference on Database Security
* INET = Internet Society Annual Conference
* IRW-FMP = International Refinement Workshop and Formal Methods Pacific
* ISCC = IEEE Symposium on Computers and Communications ISCC '98
* JCS = Journal of Computer Security
* MDDS = Mobility in Databases and Distributed Systems
* NBIS = Network-Based Information Systems
* NCISSE = National Colloquium for Information Systems Security Education
* NISS = National Information Systems Security Conference
* NSPW = New Security Paradigms Workshop NSPW
* RAID = Workshop on the Recent Advances in Intrusion Detection
* SAC = Workshop on Selected Areas of Cryptography
* SETA = Sequences and their Applications
* SICON = IEEE Singapore International Conference on Networks SICON '98
* SIGMOD/PODS - ACM SIGMOD International Conference on Management of Data
  / ACM SIGACT SIGMOD-SIGART Symposium on Principles of Database Systems
* SNDSS = Symp. on Network and Distributed System Security (Internet Society)
* USENIX Sec = USENIX Security Symposium
* VLDB = International Conference on Very Large Data Bases
* WDAG = Workshop on Distributed Algorithms (now DISC)
* WETICE = IEEE Workshops on Enabling Technologies,
  Infrastructure for Collaborative Enterprises
* WFMSP = Workshop on Formal Methods and Security Protocols

Listing of Academic (Teaching and Research) Positions in Computer Security
maintained by Cynthia Irvine

* Dept. of Electrical and Computer Engineering, Iowa State University,
  Ames, Iowa
  Assistant, Associate, or Full Professor in Computer Engineering
  (special interest in networks and security)
  Date closed: December 15, 1997, or until filled
  http://vulcan.ee.iastate.edu/~davis/job-ad.html

* Naval Postgraduate School Center for INFOSEC Studies and Research,
  Monterey, CA, Visiting Professor, (9/98)
  http://www.cs.nps.navy.mil/research/cisr/jobs/npscisr_prof_ad.html

* Naval Postgraduate School Center for INFOSEC Studies and Research,
  Monterey, CA, Computer Scientist, (9/21/97)
  http://www.cs.nps.navy.mil/research/cisr/jobs/npscisr_97de055.html

* US Air Force Academy Department of Computer Science, Colorado Springs,
  CO, Professor, (7/98)
  http://www.usafa.af.mil/dfcs/

* Purdue University, Computer Science Department, West Lafayette, IN
  Assistant Professor, tenure track, also Assoc. and Full Prof., (2/98)
  http://www.cs.purdue.edu/facAnnounce

This job listing is maintained as a service to the academic community.
If you have an academic position in computer security and would like to
have in it included on the Cipher web page and e-mail issues, send the
following information :

Institution,
City, State,
Position title,
date position announcement closes, and
URL of position description

to: irvine@cs.nps.navy.mil

How to become <<or REMAIN>> a member of the

IEEE Computer Society's TC on Security and Privacy
____

You do NOT have to join either IEEE or the IEEE Computer Society to
join the TC, and there is no cost to join the TC. All you need to do
is fill out an application form and mail or fax it to the IEEE Computer
Society. A copy of the form is included below (to simplify things,
only the TC on Security and Privacy is included, and is marked for you)
Members of the IEEE Computer Society may join the TC via an https link.
The full and complete form is available on the IEEE Computer Society's
Web Server by following the application form hyperlink at the URL:
http://computer.org/tcsignup/

IF YOU USE THE FORM BELOW, PLEASE NOTE THAT THE IT IS TO BE RETURNED
(BY MAIL OR FAX) TO THE IEEE COMPUTER SOCIETY, >>NOT<< TO CIPHER.

IEEE Computer Society
Technical Committee Membership Application

Please print clearly or type.

Last Name   First Name   Middle Initial

____

Company/Organization

____

Office Street Address (Please use street addresses over P.O.)

____

City   State

____

Country   Postal Code

____

Office Phone   Fax

____

Email Address (Internet accessible)

____

Home Address (optional)

____

Home Phone

____

[ ] I am a member of the Computer Society

IMPORTANT: IEEE Member/Affiliate/Computer Society Number:

____

[ ] I am not a member of the Computer Society*

Please Note: In some TCs only current Computer Society members are eligible to receive Technical Committee newsletters.

Please select up to four Technical Committees/Technical Councils of interest.

TECHNICAL COMMITTEES

[X] T27 Security and Privacy

Please Return Form To:
IEEE Computer Society
1730 Massachusetts Ave, NW
Washington, DC 20036-1992
Phone: (202) 371-0101
FAX: (202) 728-9614

TC Publications for Sale

Proceedings of the IEEE CS Symposium on Security and Privacy

Sorry! Strong response has reduced our stocks of old proceedings, and we have closed last year's conference books, so we will not be accepting any more orders for the present. You may still order some back issues from IEEE CS Press at http://www.computer.org/cspress/catalog/proc9.htm.

Last year's Computer Security Foundation Workshop (CSFW11) took place the 10th through 12th of June in Rockport, Massachusetts USA. Topics included formal specification of security protocols, protocol engineering, distributed systems, information flow, and security policies. Copies of the proceedings are available from the publications chair for $25 each. Copies of all earlier proceedings (except the first) are also available at $10. Checks payable to "Joshua Guttman for CSFW" may be sent to:

Joshua Guttman, MS A150
The MITRE Corporation
202 Burlington Rd.
Bedford, MA 01730-1420 USA
guttman@mitre.org

TC Officer Roster

Chair:
Charles P. Pfleeger
Arca Systems, Inc.
8229 Boone Blvd, Suite 750
Vienna VA 22182-2623
(703) 734-5611 (voice)
(703) 790-0385 (fax)
c.pfleeger@computer.org

Past Chair:
Deborah Cooper
P.O. Box 17753
Arlington, VA 22216
(703) 908-9312 (voice and fax)
d.cooper@computer.org

Vice Chair:
Thomas A. Berson
Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94301
(650) 324-0100 (voice)
berson@anagram.com

Chair, Subcommittee on Academic Affairs:
Prof. Cynthia Irvine
U.S. Naval Postgraduate School
Computer Science Department
Code CS/IC
Monterey CA 93943-5118
(408) 656-2461 (voice)
irvine@cs.nps.navy.mil

Newsletter Co-editors:

Paul Syverson
Code 5543
Naval Research Laboratory
Washington, DC 20375-5337
(202) 404-7931 (voice)
(202) 404-7942 (fax)
syverson@itd.nrl.navy.mil

Avi Rubin
AT&T Labs - Research
Room B282
180 Park Ave.
Florham Park NJ 07932-0971
(973) 360-8356 (voice)
(973) 360-8809 (fax)
rubin@research.att.com

Chair, Subcommittee on Standards:
David Aucsmith
Intel Corporation
JF2-74
2111 N.E. 25th Ave
Hillsboro OR 97124
(503) 264-5562 (voice)
(503) 264-6225 (fax)
awk@ibeam.intel.com

Chair, Subcomm. on Security Conferences:
Michael Reiter
AT&T Labs - Research
Room A269
180 Park Ave
Florham Park NJ 07932-0971
(973) 360-8349 (voice)
(973) 360-8809 (fax)
reiter@research.att.com

Information for Subscribers and Contributors

SUBSCRIPTIONS: Two options:
1. To receive the full ascii CIPHER issues as e-mail, send e-mail to
<cipher-request@itd.nrl.navy.mil>
(which is NOT automated) with subject line "subscribe".
2. To receive a short e-mail note announcing when a new issue of CIPHER
is available for Web browsing or downloading from our ftp server
send e-mail to
<cipher-request@itd.nrl.navy.mil>
(which is NOT automated) with subject line "subscribe postcard".
To remove yourself from the subscription list, send e-mail to
cipher-request@itd.nrl.navy.mil with subject line "unsubscribe".
Those with access to hypertext browsers may prefer to read Cipher that
way. It can be found at URL
http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher

CONTRIBUTIONS: to <cipher@itd.nrl.navy.mil> are invited. Cipher is a NEWSletter, not a bulletin board or forum. It has a fixed set of departments, defined by the Table of Contents. Please indicate in the subject line for which department your contribution is intended. For Calendar entries, please include a URL and/or e-mail address for the

point-of-contact. For Calls for Papers, please submit a one paragraph
summary. See this and past issues for examples. ALL CONTRIBUTIONS
CONSIDERED AS PERSONAL COMMENTS; USUAL DISCLAIMERS APPLY. All
reuses
of Cipher material should respect stated copyright notices, and should
cite the sources explicitly; as a courtesy, publications using Cipher
material should obtain permission from the contributors.

BACK ISSUES:

There is an archive that includes each copy distributed so far, in ascii,
in files you can download at URL
http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html
There is also an anonymous FTP server that contains the same files.
To access the archive via anonymous FTP:

1. ftp www.itd.nrl.navy.mil
2. At prompt for ID, enter "anonymous"
3. At prompt for password, enter your actual, full e-mail address
4. Once you are logged in, change to the Cipher Directory:
   cd pub/cipher
5. Now you can request any of the files containing Cipher issues in ascii.
   Issues are named in the form: EI#N.9708 where N is the number of the
   issue desired and 9703 captures the year and month it appeared.

=========end of Electronic Cipher Issue #27, 27 April 1998==============